BinGO!

User´s Guide

Installation und Konfiguration

Ziel und Zweck

Dieses Handbuch beschreibt die Installation und Erstkonfiguration von **BinGO!** mit Software-Release 4.9.3. Für neueste Informationen und Hinweise zum aktuellen Software-Release sollten Sie in jedem Fall zusätzlich unsere Release Note lesen – insbesondere, wenn Sie ein Software-Update zu einem höheren Release-Stand durchführen. Die aktuellste Release Note ist immer zu finden unter www.bintec.de.

Haftung

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

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

Als ISDN-Multiprotokollrouter baut **BinGO!** in Abhängigkeit von der Systemkonfiguration ISDN-Verbindungen auf. Um ungewollte Gebühren zu vermeiden, sollten Sie das Produkt unbedingt überwachen. BinTec Communications AG übernimmt keine Verantwortung für Datenverlust, ungewollte Verbindungskosten und Schäden, die durch den unbeaufsichtigten Betrieb des Produkts entstanden sind.

Marken

BinTec und das BinTec-Logo sind eingetragene Warenzeichen der BinTec Communications AG.

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

Copyright

Richtlinien und Normen

BinGO! entspricht folgenden Richtlinien und Normen:

- Niederspannungsrichtlinie 73/23/EWG nach EN60950
- Gerätesicherheit

- Störfestigkeit nach EN50082 -1/1.32
- Störaussendung Grenzwertklasse B nach EN55022 /-8.94
- Elektromagnetische Verträglichkeit nach EU-Richtlinie 89/336/EWG
- CE-Zeichen für alle EG-Länder

Zulassungen:

- BZT D 133451J (CE und deutsche Zulassung)
- BZT D 133457J (EG-Baumusterprüfbescheinigung)
- BAKOM (gemeldet)
- CE 0188X (Frankreich erkennt die CE-Zulassung an)
- EN50082, EN55022
- EN60950

Zusätzlich zu den CE-Richtlinien genügt **BinGO!** den ISDN-Voraussetzungen in Frankreich und kann an Euro-Numeris angeschlossen werden.

Wie Sie BinTec erreichen

Über ...	Unter der Telefonnummer oder Adresse
Telefon	+49 911 96 73 0
Fax	+49 911 688 07 25
Brief	BinTec Communications AG Südwestpark 94 D-90449 Nürnberg
Internet	www.bintec.de

Version 1.0
Dokument #70000B
März 1999

Inhaltsübersicht

1 Willkommen!

Wir dürfen Sie zum Kauf Ihres Personal ISDN Internet Access Routers von BinTec Communications AG beglückwünschen. Damit haben Sie ein erfolgreiches Produkt von BinTec Communications AG aus unserer Produktgruppe Personal Access erworben. Dieser leistungsstarke Multiprotokollrouter ermöglicht Ihnen die kostengünstige Vernetzung kleiner Netzwerke. **BinGO!** wird Ihnen in Zukunft die Anbindung Ihres Einzelarbeitsplatzes oder kleinen Unternehmens an das Internet und an andere Partnernetze (z. B. eine Firmenzentrale) ermöglichen. **BinGO!** wird Ihnen außerdem moderne Mittel der Bürokommunikation (Kommunikationsanwendungen wie z. B. Fax und Filetransfer) netzwerkweit an jedem Rechner verfügbar machen.

Wie geht's weiter?

Was Sie an BinGO! haben... ..., was **BinGO!** für Sie bedeutet und was **BinGO!** alles kann, erfahren Sie auf den folgenden Seiten.

Wie Sie BinGO! das Laufen lehren... ...erfahren Sie im Kapitel 3, Seite 35. Dort zeigen wir Ihnen, wie Sie **BinGO!** innerhalb weniger Minuten von einem Windows-PC aus mit einem Konfigurations-Assistenten in Betrieb nehmen und wie Sie weitere nützliche Hilfsprogramme installieren. Am Ende dieses Kapitels sind Sie in der Lage, im Internet zu surfen, E-Mails oder Faxe zu verschicken und zu empfangen und eine Verbindung mit einem Partnernetz herzustellen, um beispielsweise auf Daten einer Firmenzentrale zuzugreifen.

Was Sie sonst noch alles tun können... ...erklären wir ausführlich ab Kapitel 6, Seite 123. Dort erfahren Sie alle Konfigurationsmöglichkeiten im Detail. Auch wenn Sie keinen Windows-PC haben, werden Sie dort schnelle Wege finden, **BinGO!** zu konfigurieren.

Wenn Sie bereits BinTec-Router konfiguriert haben...

..., Sie sich mit der Konfiguration gut auskennen und gleich loslegen wollen, fehlen Ihnen eigentlich nur noch der werkseitig eingestellte Benutzername und das Paßwort:

Benutzername	Paßwort
admin	bintec

Aber denken Sie daran, das Paßwort sofort zu ändern, wenn Sie sich das erste mal auf **BinGO!** einloggen. Alle BinTec-Router werden mit gleichem Paßwort ausgeliefert. Sie sind daher erst gegen einen unautorisierten Zugriff geschützt, wenn Sie das Paßwort ändern.

Ansonsten...

... wünscht BinTec Communications AG Ihnen viel Spaß mit Ihrem neuen Produkt.

1.1 Wozu BinGO!?

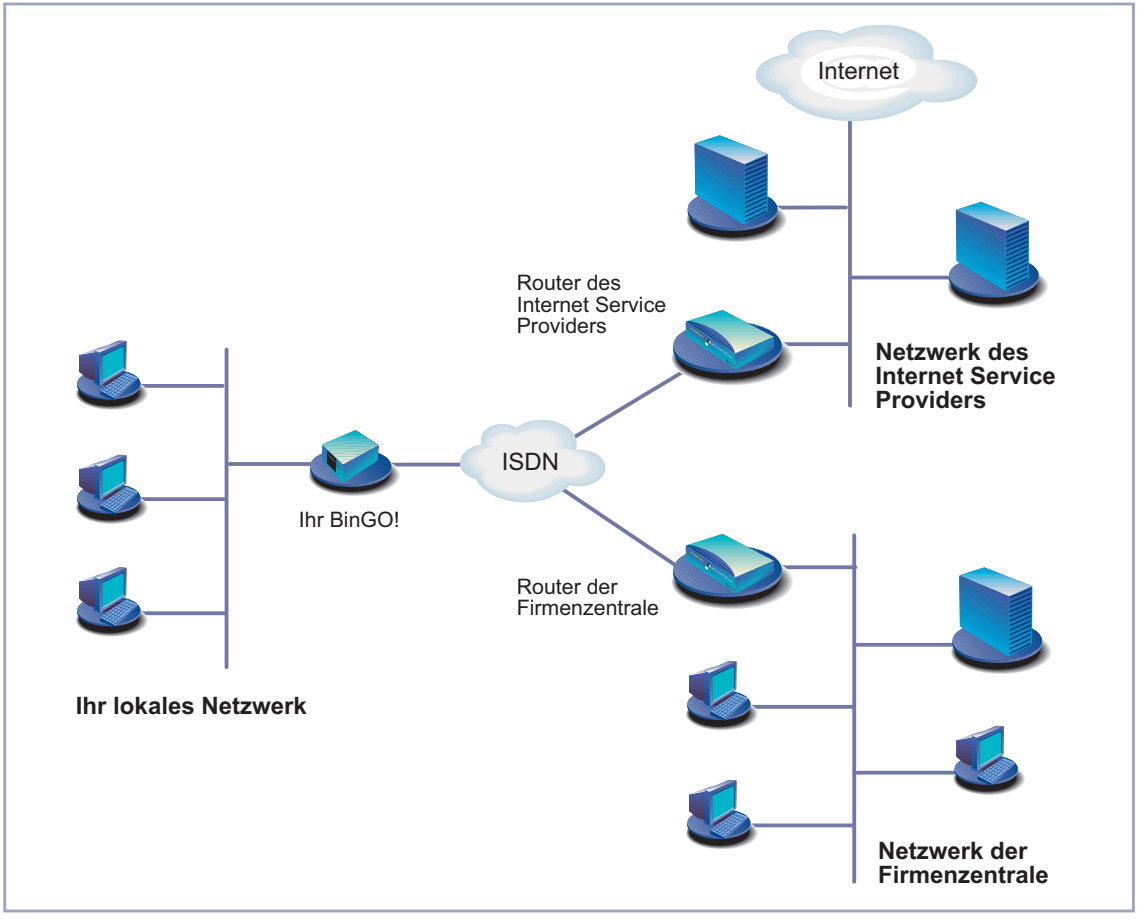


Bild 1-1: Grundszenario

Wozu Router wie BinGO!?

Router werden verwendet, um Netzwerke miteinander zu verbinden und um Informationen zwischen den Netzwerken auszutauschen. So können Sie beispielsweise wie im Bild oben über Ihren Router eine Verbindung mit dem Netz Ihres Internet Service Providers herstellen und dadurch die gängigen Dienste des Internet nutzen, wie das World Wide Web (WWW) oder E-Mail. Über eine Verbindung zu einem anderen Partnernetz, z. B. Ihrer Firmenzentrale, können

Sie bequem von Ihrem Heimarbeitsplatz oder von einer Filiale aus auf alle Informationen der Zentrale zugreifen, auch wenn diese geographisch weit entfernt liegt. Die Verbindung dieser lokalen Netze erfolgt über das ISDN. Wie groß dabei Ihr eigenes lokales Netzwerk ist – ob es aus mehreren Rechnern besteht oder ob es sich um einen Einzelarbeitsplatz handelt – spielt prinzipiell keine Rolle.

Wie aus vorheriger Abbildung ersichtlich ist, ist **BinGO!** für eine Verbindung der Netzwerke die entscheidende Komponente: Ihr Router ist die Verbindung zur Außenwelt. Jeder Router ist in der Abbildung über den ISDN-Anschluß an das ISDN gekoppelt und dient so als Bindeglied zwischen den einzelnen lokalen Netzwerken. Innerhalb jedes einzelnen Netzwerks (LAN) ist der Router wie ein normaler Rechner an das Netzwerk angeschlossen. Er hat die Aufgabe, gegebenfalls Informationen aus dem eigenen Netz nach außen an ein anderes Netz (z. B. an das Netz Ihres Internet Service Providers oder das Netz einer Firmenzentrale) weiterzuleiten und dafür die geeigneten Wege (Routen) zu finden. Umgekehrt empfängt er Informationen und routet diese ins eigene Netz weiter.

Was kann **BinGO!**, was Modem oder ISDN-Karte nicht könnten? Ihr **BinGO!** bietet weitaus mehr:

Ein Router für alle

Wenn Sie ein lokales Netzwerk mit mehreren Rechnern haben, brauchen Sie nur einen einzigen Router, um allen Rechnern im Netz den Zugriff auf das Internet oder die Firmenzentrale zu ermöglichen. Dies bedeutet bei mehreren Rechnern im Netz eine erhebliche Kostenersparnis, da Sie sowohl weniger an Ausstattung als auch an Wartung investieren. Bei Einsatz von Modems oder ISDN-Karten müßten Sie jeden Arbeitsplatz einzeln ausstatten.

Kommunikationsanwendungen

Das Gleiche gilt für Kommunikationsanwendungen wie z. B. Anrufbeantworter, Fax, Dateitransfer und Euro-Filetransfer, die Sie von Ihrem Rechner aus bedienen. Über eine BinTec-eigene Schnittstelle, die Remote-CAPI, können alle Teilnehmer im LAN diese Dienste nutzen, dabei aber über **BinGO!** auf einen einzigen ISDN-Anschluß zugreifen. Voraussetzung ist, daß alle Teilnehmer eine geeignete Anwendungssoftware installiert haben, die die sogenannte CAPI-Schnittstelle unterstützt. Diese genormte Schnittstelle wird von den meisten Kommunikationsanwendungen verwendet. Im Lieferumfang von **BinGO!** ist eine entsprechende Software enthalten, RVS-COM Lite. Mit ihr decken Sie das Spektrum der gängigen Kommunikationsanwendungen ab.

Automatisches Einwählen und Beenden

Ein wesentlicher Vorteil von **BinGO!** zeigt sich außerdem in der Zugangsart. Ihr Router entscheidet – einmal konfiguriert – selbständig, ob und wie er eine Verbindung zum Internet Service Provider herstellen muß. Sie geben zum Beispiel in Ihren Browser eine externe WWW-Adresse ein, **BinGO!** stellt fest, daß die angeforderte Adresse außerhalb Ihres eigenen LANs liegt und baut die Verbindung zu Ihrem Internet Service Provider und somit dem Internet automatisch auf. Und – damit Sie Kosten sparen – beendet **BinGO!** die Verbindung nach einer definierten Zeit (Shorthold) wieder, wenn keine Informationen mehr ausgetauscht werden.

Das gleiche Prinzip wenden Sie an, um auf Daten eines anderen Standortes, z. B. Ihrer Firmenzentrale, bequem zuzugreifen. Sie können sogar unter Windows ein Netzlaufwerk mit einem Rechner der Firmenzentrale verbinden. Im Windows-Explorer klicken Sie dann einfach auf das Symbol dieser Verknüpfung und "surfen" in den Verzeichnissen und Daten des entfernten Rechners wie auf Ihrer eigenen Festplatte. Um den Auf- und Abbau der Verbindung kümmert sich **BinGO!**.

Sicherheit

Auch in puncto Sicherheit bietet **BinGO!** einiges. Mit Ihrem Router besitzen Sie integrierte Firewall-Mechanismen. Ihr Router erfüllt alle Anforderungen bezüglich Zugangssicherheit umfangreich und kostengünstig. Er schirmt Ihr Netz gegen unbefugten Zugriff von außen ab. Dies wird möglich durch **BinGO!**'s SAFERNET-Funktionen wie Verschlüsselung, Filter, Monitoring.

Konfiguration und Wartung

Für die Konfiguration von **BinGO!** bieten sich eine Reihe von Optionen. Die meisten Konfigurationsmethoden sind unabhängig vom Betriebssystem Ihres Rechners.

Die einfachste Methode unter Windows ist der Configuration Wizard. Dieser Konfigurations-Assistent leitet Sie Schritt für Schritt durch die Konfiguration und unterstützt Sie, die wichtigsten Einstellungen an Ihrem Router vorzunehmen. In wenigen Minuten ist **BinGO!** einsatzbereit.

BinGO! ist außerdem fernkonfigurier- und fernwartbar. Sobald Ihr Router – selbst im Auslieferungszustand – an das ISDN angeschlossen ist, können von einem anderen Standort aus (z. B. als Administrator einer Firmenzentrale) Konfigurationseinstellungen vorgenommen werden. Die Einrichtung des Systems können Sie so einem Verantwortlichen in der Zentrale überlassen.

Zusammenfassend Die Hauptvorteile von **BinGO!** lassen sich wie folgt zusammenfassen:

- Eine Verbindung mit dem Internet oder einem anderen Partnernetz, damit alle im LAN die gängigen Internetdienste nutzen (z. B. E-Mail, WWW, Filetransfer) und auf Daten anderer Standorte zugreifen können.
- Eine gemeinsame Nutzung von Kommunikationsanwendungen im LAN (z. B. Fax, Anrufbeantworter).
- Einfache Konfiguration für Sie und Fernwartung durch einen Administrator.
- Unabhängigkeit vom Betriebssystem Ihres Rechners.

Dabei müssen Sie auf Sicherheit, Bequemlichkeit und Kostenkontrolle nicht verzichten.

1.2 Lieferumfang

BinGO! wird zusammen mit folgenden Teilen ausgeliefert:

- Kabelsätze/Netzteil:
  - Je ein Kabel (RJ45) für LAN- und ISDN-Anschluß
  - Serielles Anschlußkabel
  - Adapter für serielles Anschlußkabel
  - Steckernetzteil
- BinTec Companion CD
- Dokumentation:
  - User’s Guide
  - Release Note, falls erforderlich
- Beipackzettel:
  - Quick Install Guide (englisch)
  - Kurzanleitung (deutsch)
  - Lizenzinformation
  - Lizenzkarte

1.3 BinTec Companion CD

Auf Ihrer BinTec Companion CD finden Sie alle Programme, die Sie zur Installation, Konfiguration und Wartung von **BinGO!** brauchen.

BRICKware

- Die DIME Tools dienen der Überwachung und Administration von **BinGO!**.
- Der Configuration Wizard führt Sie Schritt für Schritt durch die Grundkonfiguration von **BinGO!**.
- Über das Terminal Programm BRICK at COM1 bzw. BRICK at COM2 erhalten Sie Zugang zu **BinGO!** über die serielle Schnittstelle.
- Der DIME Browser erlaubt es Ihnen, alle BinTec-Router im Netz über eine graphische Oberfläche zu konfigurieren und administrieren. Hier können Sie alle SNMP-Tabellen und -Variablen einsehen und bearbeiten.
- Mit dem JAVA Statusmonitor können Sie über einen Internet Browser alle relevanten Systeminformationen abfragen.
- Remote-CAPI-Client:
  Mit dem Remote-CAPI-Client können Sie Kommunikationsanwendungen nutzen, die auf die genormte CAPI-Schnittstelle aufsetzen (z. B. RVS-COM Lite).
- Token Authentication Firewall (TAF) Programm:
  Dieses Softwarepaket benötigen Sie, wenn Sie das Sicherheitssystem von Security Dynamics verwenden.

Genauere Beschreibungen aller Softwareprogramme finden Sie in unserem Online-Handbuch BRICKware for Windows.

RVS-COM Lite

Zusätzlich zur BRICKware ist auf Ihrer BinTec Companion CD das Kommunikationsprogramm RVS-COM Lite enthalten, das Ihnen typische Kommunikationsanwendungen wie z. B. Anrufbeantworter, Fax oder Dateitransfer auf Ihrem Rechner ermöglicht. Wie erklären wir in Kapitel 3.7, Seite 68.

Was sonst?

Wenn Sie die Companion CD durchsuchen, stoßen Sie auf eine Reihe weiterer nützlicher Verzeichnisse, in denen Sie z. B. finden:

- Die Dokumentation in elektronischer Form (siehe Kapitel 1.4, Seite 22)

- Eine Kopie der Router-Software (Auslieferungszustand)
- UNIX-Tools
- Adobe’s Acrobat Reader
- Konfigurationsbeispiele

1.4 Dokumentation bei BinTec

Die Dokumentation haben Sie zusammen mit **BinGO!** teilweise in gedruckter und komplett in elektronischer Form (PDF, HTML) erhalten. Die elektronischen Fassungen der verschiedenen Dokumente finden Sie auf Ihrer BinTec Companion CD. Zusätzlich zur Companion CD stehen alle Dokumente jeweils in der aktuellsten Version auf unserem WWW-Server unter www.bintec.de zum Download bereit. Es gibt:

- User's Guide (deutsch und englisch, PDF bzw. gedruckt):
  Dieses Handbuch. Die deutsche Version steht nur in elektronischer Fassung (PDF) zur Verfügung und kann bei Bedarf ausgedruckt werden.
- Faltblätter, um **BinGO!** in wenigen Minuten in Betrieb zu nehmen (PDF und gedruckt):
  - Quick Install Guide (englisch)
  - Kurzanleitung (deutsch)
- Referenzhandbücher (englisch, PDF/HTML):
  - Software Reference (PDF)
    Online-Nachschlagewerk mit tiefergehenden Informationen zu hier beschriebenen Funktionen, Nachschlagewerk für die internen SNMP-Tabellenstrukturen und die Bedienung der SNMP-Shell.
  - Extended Feature Reference (PDF)
    Online-Nachschlagewerk für zusätzliche, nur mit separater Lizenz verfügbare Funktionen (z. B. VPN).
  - MIB Reference
    HTML-Dokument mit Kurzbeschreibungen zu allen SNMP-Tabellen und Variablen von **BinGO!**.
- BRICKware for Windows (englisch, PDF):
  Bedienungsanleitung für die Windows-Hilfsprogramme (BRICKware)
- Release Notes (englisch, PDF und/oder gedruckt):
  Aktuelle Informationen und Hinweise zum aktuellen Software-Release, Beschreibung aller Änderungen gegenüber dem vorherigen Release.
  Im Dokument Release Note Logic finden Sie eine Anleitung zum Upgrade von Bootmonitor und/oder Firmware-Logic.

- UK Info (englisch, PDF):
  Hinweise zum Betrieb von BinTec Routern in Großbritannien.

1.5 Systemvoraussetzungen

BinGO! können Sie von allen herkömmlichen Plattformen aus konfigurieren. Als Standalone-Gerät ist **BinGO!** nicht vom angeschlossenen Rechner oder dessen Betriebssystem abhängig. Die Kommunikation zum Rechner erfolgt über eine LAN-Schnittstelle (10 MBit/s) oder einen seriellen Anschluß. Somit kann Ihr Router in den verschiedensten Betriebssystemumgebungen wie DOS, Windows, UNIX, AS/400, Macintosh oder Novell eingesetzt werden.

Speziell für die Verwendung des Configuration Wizard benötigen Sie:

- Rechner mit serieller Schnittstelle (V.24)
- Windows 95 bzw. 98 oder Windows NT 4.0
- Installierte Netzwerkkarte (10 MBit/s Ethernet)
- Installiertes Microsoft TCP/IP-Protokoll
  Wie Sie herausfinden, ob Ihr Rechner über die nötigen Einstellungen verfügt und wie Sie gegebenenfalls die Einstellungen selbst vornehmen, erklären wir Ihnen, bevor Sie mit der Konfiguration loslegen.
- High Color Monitor (mindestens 32000 Farben) für die korrekte Darstellung der Grafiken

1.6 Garantiebedingungen

BinGO! hat 36 Monate Garantie ab Kaufdatum. Zur Garantieabwicklung wenden Sie sich bitte an Ihren Händler.

1.7 Zu diesem Handbuch

1.7.1 Inhalt

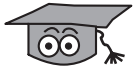
Das Handbuch ist folgendermaßen aufgebaut:

Kapitel	Inhalt
1: Willkommen!	Allgemeine Einführung, Lieferumfang, Garantiebedingungen, Informationen zu diesem Handbuch.
2: Allgemeine Sicherheitshinweise	Allgemeine Sicherheitshinweise in deutsch.
3: Los geht's	Anweisungen, wie Sie **BinGO!** mit dem Configuration Wizard in wenigen Minuten in Betrieb nehmen und wie Sie weitere nützliche Software installieren und einrichten.
4: Grundlagen	Wichtige Grundlagen zum Thema Router und Netzwerke.
5: Ein Draht zu BinGO!	Grundlagen zum Umgang mit dem Setup Tool.
6: Grundkonfiguration mit Setup Tool	Wie Sie **BinGO!** mit dem Setup Tool (analog zum Configuration Wizard) in Betrieb nehmen.
7: Weiterführende Konfiguration	Wie Sie weitere Konfigurationseinstellungen mit dem Setup Tool vornehmen.
8: Sicherheitsmechanismen	Wie Sie Sicherheitsmechanismen gemäß SAFERNET einrichten, z. B. NAT (Network Address Translation) oder CLID (Calling Line Identification).
9: Konfigurationsmanagement	Wie Sie Konfigurationsdateien verwalten und wie Sie Software-Updates durchführen.
10: Troubleshooting	Wichtige Hinweise zur Fehlerbehebung.
11: Technische Daten	Die Technischen Daten von **BinGO!.**

Kapitel	Inhalt
12: Wichtige Kommandos	Eine Kurzübersicht zu den wichtigsten Befehlen und Kommandos der SNMP-Shell und der BRICKtools für Unix.
13: Allgemeine Sicherheitshinweise in 15 verschiedenen Sprachen	Allgemeine Sicherheitshinweise in den unterschiedlichen Fremdsprachen.

1.7.2 Verwendung

Damit Sie wichtige Informationen in diesem Handbuch besser finden, werden folgende Symbole verwendet:

Symbol	Verwendung
	Kennzeichnet Stellen, an denen Tips und Tricks verraten werden.
	Kennzeichnet Stellen, an denen Hinweise zur Fehlerbehebung gegeben werden.
	Kennzeichnet allgemeine wichtige Hinweise.
	Kennzeichnet Stellen, an denen wichtige Grundlagen erläutert werden.

Symbol	Verwendung
	Kennzeichnet Warnhinweise. Einteilung der Gefahrenstufen gemäß ANSI: ■ Achtung (weist auf mögliche Gefahr hin, die bei Nichtbeachten Sachschäden zur Folge haben kann) ■ Warnung (weist auf mögliche Gefahr hin, die bei Nichtbeachten Körperverletzung zur Folge haben kann) ■ Gefahr (weist auf Gefahr hin, die bei Nichtbeachten Tod oder schwere Körperverletzung zur Folge haben wird)

Damit Sie die Informationen in diesem Handbuch besser einordnen und interpretieren können, werden folgende Auszeichnungselemente verwendet:

Auszeichnung	Verwendung
➤	Hier werden Sie aufgefordert, etwas zu tun.
■ –	Listen bis zur zweiten Gliederungsebene.
MENÜ ➧ ***UNTERMENÜ***	Kennzeichnung von Menüs und Untermenüs im Setup Tool.
`nicht-proportional (Courier), z. B.` `ping 192.168.1.254`	■ Kennzeichnung von Kommandos (z. B. in der SNMP-Shell), die Sie wie dargestellt eingeben müssen. ■ Darstellung des Setup Tool.
fett, kursiv, z. B. ***BigBoss***	Kennzeichnung von Beispielbegriffen.
fett, z. B. ➤➤ **MIB**	Kennzeichnung von Begriffen, die Sie im Glossar finden (Online ist der Doppelpfeil klickbar).
fett, z. B. **biboAdmLoginTable,** **Windows-Startmenü**	■ Kennzeichnung von Feldern im Setup Tool und MIB-Tabellen/-Variablen. ■ Kennzeichnung von Tasten/Tastenkombinationen und Windows-Begriffen.
kursiv, z. B. *none*	Kennzeichnung von Werten, die Sie im Setup Tool oder bei MIB-Variablen eintragen bzw. eingestellt werden können.
Online: unterstrichen	Kennzeichnung von Links.

1 Willkommen!

2 Allgemeine Sicherheitshinweise

In den nachfolgenden Abschnitten finden Sie Sicherheitshinweise, die Sie beim Umgang mit Ihrem Router unbedingt beachten müssen.

Transport und Lagerung

- Transportieren und lagern Sie **BinGO!** nur in der Originalverpackung oder in einer anderen geeigneten Verpackung, die Schutz gegen Stoß und Schlag gewährt.

Aufstellen und in Betrieb nehmen

- Beachten Sie vor dem Aufstellen und Betrieb von **BinGO!** die Hinweise für die Umgebungsbedingungen (vgl. Technische Daten). Verwenden Sie eine feste und ebene Unterlage.
- Wenn das Gerät aus kalter Umgebung in den Betriebsraum gebracht wird, kann Betauung sowohl am Geräteäußeren als auch im Geräteinneren auftreten. Warten Sie, bis Ihr Router temperaturangeglichen und absolut trokken ist, bevor Sie ihn in Betrieb nehmen.
- Überprüfen Sie, ob die auf dem Typenschild des Netzteils angegebene Nennspannung mit der örtlichen Netzspannung übereinstimmt. **BinGO!** darf nur mit dem original BinTec Communications-Steckernetzteil (5 V DC) betrieben werden. BinTec Communications AG haftet nicht für Schäden, die durch die Verwendung eines anderen Steckernetzteils hervorgerufen werden.
- Beachten Sie beim Verkabeln die Reihenfolge, wie im Handbuch beschrieben. Verkabeln Sie zuerst LAN-, ISDN- und serielle Anschlüsse, schließen Sie dann die Stromversorgung an, und schalten Sie zum Schluß **BinGO!** ein.
- Überprüfen Sie, ob Sie die Verkabelung – insbesondere die ISDN- und LAN-Verkabelung – richtig durchgeführt haben, bevor Sie **BinGO!** in Betrieb nehmen. Der ISDN-Anschluß von **BinGO!** darf nicht mit dem Ethernet-Anschluß Ihres Rechners oder Hubs verbunden werden, der LAN-Anschluß von **BinGO!** nicht mit Ihrem ISDN-Anschluß.
- Verwenden Sie für die Verkabelung nur die beigelegten Kabel. Falls Sie andere Kabel verwenden, übernimmt BinTec Communications AG für auftretende Schäden keine Haftung.

- Verlegen Sie Leitungen so, daß sie keine Gefahrenquelle (Stolpergefahr) bilden und nicht beschädigt werden.
- Schließen Sie Datenübertragungsleitungen während eines Gewitters weder an noch ziehen Sie sie ab.

Bestimmungsgemäße Verwendung, Betrieb

- **BinGO!** ist für den Einsatz in einer Büroumgebung bestimmt. Als ISDN-Multi-Protokoll-Router baut **BinGO!** in Abhängigkeit von der Systemkonfiguration ISDN-Verbindungen auf. Um ungewollte Gebühren zu vermeiden, sollten Sie das Produkt unbedingt überwachen.
- **BinGO!** entspricht den einschlägigen Sicherheitsbestimmungen für Einrichtungen der Informationstechnik für den Einsatz in einer Büroumgebung.
- Der bestimmungsgemäße Betrieb gemäß IEC 950/EN 60950 des Systems ist nur bei montiertem Gehäusedeckel gewährleistet (Kühlung, Brandschutz, Funkentstörung)
- Die Umgebungstemperatur sollte 50˚C nicht übersteigen. Vermeiden Sie direkte Sonneneinstrahlung.
- Achten Sie darauf, daß keine Gegenstände (z. B. Büroklammern) oder Flüssigkeiten ins Innere des Geräts gelangen (elektrischer Schlag, Kurzschluß). Achten Sie auf ausreichende Kühlung.
- Unterbrechen Sie in Notfällen (z. B. geschädigtes Gehäuse oder Bedienelement, Eindringen von Flüssigkeit oder Fremdkörpern) sofort die Stromversorgung und verständigen Sie den Service.

Reinigung und Reparatur

- Das Gerät darf nur durch geschultes Fachpersonal geöffnet werden. Lassen Sie daher Reparaturen am Gerät nur von einer BinTec-autorisierten Servicestelle durchführen. Wo sich die Servicestelle befindet, erfahren Sie von Ihrem Händler. Durch unbefugtes Öffnen und unsachgemäße Reparaturen können erhebliche Gefahren für den Benutzer entstehen (z. B. Stromschlag). Unerlaubtes Öffnen der Geräte hat den Garantie- und Haftungsausschluß der BinTec Communications AG zur Folge.
- Das Gerät darf auf keinen Fall naß gereinigt werden. Durch eindringendes Wasser können erhebliche Gefahren für den Benutzer (z. B. Stromschlag) und erhebliche Schäden am Gerät entstehen.

- Niemals Scheuermittel, alkalische Reinigungsmittel, scharfe oder scheuernde Hilfsmittel benutzen.

2 Allgemeine Sicherheitshinweise

3 Los geht’s

Dieses Kapitel hilft Ihnen, so schnell wie möglich die wichtigsten und gängigen Anwendungen für Ihr lokales Netzwerk oder Ihren Einzelarbeitsplatz zu konfigurieren. Um Ihnen die Konfiguration so einfach wie möglich zu machen, unterstützt Sie ein Konfigurations-Assistent, Ihr **Configuration Wizard**. Mit Ihm haben Sie **BinGO!** in wenigen Minuten konfiguriert.

Am Ende dieses Kapitels können Sie:

- **BinGO!** im LAN erreichen
- Im Internet surfen
- Faxe verschicken und empfangen
- Bei Bedarf eine Verbindung mit einem entfernten Netzwerk herstellen (LAN-LAN-Kopplung, z. B. Ihre Firmenzentrale), um bequem von zu Hause aus auf Daten der Zentrale zuzugreifen

Um diese Anwendungen einzurichten, müssen Sie:

- **BinGO!** zunächst aufstellen und anschließen (Kapitel 3.1, Seite 37)
- Einige Vorbereitungen treffen (Kapitel 3.2, Seite 40)
- Windows-Software installieren und einrichten:
  - BRICKware for Windows installieren (Kapitel 3.3, Seite 46)
  - **BinGO!** mit dem Configuration Wizard konfigurieren (Kapitel 3.4, Seite 48)
  - Remote-CAPI-Schnittstelle konfigurieren (Kapitel 3.5, Seite 61)
- Eventuell zusätzliche Einstellungen an Ihren Rechnern vornehmen (Kapitel 3.6, Seite 63)
- RVS-COM Lite installieren und einrichten (Kapitel 3.7, Seite 68)

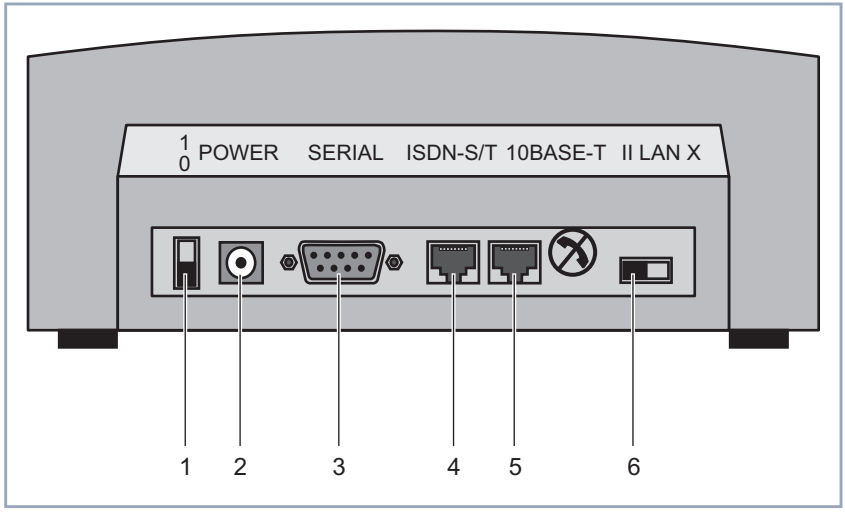
Am Ende des Kapitels erklären wir Ihnen, wie Sie Ihre Konfiguration testen.

Wie Sie Ihre Konfiguration nach Abschluß der Grundkonfiguration weiter verbessern, finden Sie ab Kapitel 7, Seite 189.

Wenn Sie sich fragen, wie Sie Ihre Grundkonfiguration ohne den Configuration Wizard einrichten (z. B. weil Sie kein Windows-Betriebssystem verwenden), lesen Sie Kapitel 6, Seite 123.

Dieses Kapitel hält Sie nicht unnötig mit technischen Details von einer raschen Konfiguration ab. Wenn Sie aber später trotzdem einige Hintergrundinformationen wissen wollen, dann lesen Sie Kapitel 4, Seite 79.

3.1 Aufstellen und Anschließen



1	Ein-/Ausschalter	4	S_0-Schnittstelle (ISDN)
2	Stromversorgungsanschluß	5	10Base-T Schnittstelle (LAN)
3	Serielle Schnittstelle	6	LAN-Schalter

Bild 3-1: **BinGO!** Rückansicht

BinGO! können Sie wahlweise an die Netzwerkkarte Ihres Rechners oder an einen Hub anschließen, wenn Sie ein kleines Netzwerk besitzen. Sie müssen hierfür lediglich den LAN-Schalter (6) an der Geräterückseite entsprechend einstellen. Wie erfahren Sie nachfolgend.

Über den ISDN-S/T-Anschluß (4) verbinden Sie **BinGO!** mit dem ISDN. Ob Sie eine ISDN-Anschlußdose, einen ➤➤ **NTBA-Adapter** oder eine TK-Anlage verwenden, macht für **BinGO!** keinen Unterschied. Wollen Sie jedoch TK-Anlagen-spezifische Funktionen nutzen, schließen Sie **BinGO!** an die TK-Anlage an. So können Sie z. B. Rufnummern sperren, die dann bei **BinGO!** gar nicht erst ankommen. Oder Sie kontrollieren die Gebühren der Rufnummern, die Sie **BinGO!** zuweisen.

Achtung!

Die Verwendung eines falschen Netzadapters kann zum Defekt Ihres Routers führen!

- Verwenden Sie ausschließlich das mitgelieferte Steckernetzteil (5 V DC).
- Vergewissern Sie sich, daß die auf dem Steckernetzteil vermerkte Nennspannung mit der lokalen Spannungsversorgung übereinstimmt.
- Tauschen Sie niemals die Netzadapter von **BinGO!** und **BinGO! Plus/Professional** aus.

Achtung!

Bei falscher Verkabelung der ISDN- und LAN-Schnittstellen kann es zum Defekt Ihres Routers kommen.

- Verbinden Sie immer nur die LAN-Schnittstelle von **BinGO!** mit der LAN-Schnittstelle des Rechners/Hubs und die ISDN-Schnittstelle von **BinGO!** mit dem ISDN-Anschluß.

Gehen Sie beim Anschließen in folgender Reihenfolge vor:

- Stellen Sie **BinGO!** auf eine feste, ebene Unterlage.

- Stellen Sie den LAN-Schalter (6) auf:
  - || wenn Sie **BinGO!** an Ihren LAN-Hub anschließen (vgl. Bild 3-1, Seite 37)
  - X wenn Sie **BinGO!** nicht an ein LAN anschließen (weil Sie keinen Hub haben), sondern direkt mit der Netzwerkkarte Ihres Rechners verbinden (Einzelarbeitsplatz).

  Durch die Verwendung des Node-/Hub-Umschalters (6) können Sie in jedem Fall das mitgelieferte 1 zu 1 verdrahtete Kabel verwenden. Ein LAN-Kabel mit gekreuzten Adern (Cross-Over-Kabel) ist nicht erforderlich.

- Verbinden Sie die serielle Schnittstelle Ihres Rechners (COM1 oder COM2) mit der seriellen Schnittstelle des Routers (3). Verwenden Sie dazu das mitgelieferte serielle Kabel und gegebenenfalls den Adapter (9-polig auf 25-polig).

- Verbinden Sie **BinGO!** mit Ihrem Hub oder mit der Netzwerkkarte Ihres Rechners (Einzelarbeitsplatz). Verwenden Sie dazu eines der mitgelieferten Kabel (RJ-45) an der 10Base-T-Schnittstelle (5).

- Verbinden Sie die S_0-Schnittstelle des Routers (4) über das zweite mitgelieferten Kabel (RJ-45) mit Ihrem ISDN-Anschluß.

- Schließen Sie **BinGO!** über die Stromversorgung (2) mit dem mitgelieferten Netzadapter an eine Steckdose an.

- Schalten Sie den Router mit dem Ein-/Ausschalter (1) ein.

  BinGO! führt einen Selbsttest durch. Wenn Sie alle Kabel richtig angeschlossen haben, erlischt die rote LED ERR am Ende des Selbsttests; die grüne LED PWR (Betriebsanzeige) leuchtet.

3.2 Konfiguration vorbereiten

3.2.1 Daten sammeln

Bevor Sie gleich mit der Konfiguration loslegen, sollten Sie Daten für folgende Zwecke bereitlegen – je nachdem, was Sie mit **BinGO!** machen wollen:

- Router-Grundkonfiguration mit Lizenzierung (obligatorisch)
- Internetzugang (optional)
- Firmennetzanbindung (optional)

In den folgenden Tabellen haben wir jeweils Beispiele angegeben, wie die Werte zu den benötigten Zugangsdaten lauten könnten. Unter der Rubrik "Ihr Wert" sollten Sie Ihre persönlichen Daten ergänzen. Dann haben Sie diese bei Bedarf griffbereit.

Router-Grundkonfiguration

Für eine Grundkonfiguration von **BinGO!** benötigen Sie Informationen, die Ihren ISDN-Anschluß und Ihre Netzwerkumgebung betreffen:

Zugangsdaten	Beispielswert	Ihre Werte
ISDN-Rufnummern Die ISDN-Rufnummern erhalten Sie mit Ihrem ISDN-Anschluß.	***967310*** ***967311*** ***967312***	
BinGO! IP-Adresse	***192.168.1.254***	
BinGO! Netzmaske	***255.255.255.0***	

Im Folgenden beschreiben wir die Einstellungen für den Anschluß von **BinGO!** am NTBA-Adapter. Beim Anschluß an eine TK-Anlage beachten Sie die Besonderheiten Ihres Anschlusses und lesen Sie gegebenenfalls in der Dokumentation Ihrer TK-Anlage nach.

Wenn Sie bisher kein Netzwerk haben und nicht wissen, wie Sie IP-Adressen und Netzmaske in einem neuen Netzwerk vergeben müssen, dann übernehmen Sie einfach die angegebenen Beispielwerte. Ansonsten fragen Sie Ihren System-Administrator.

Für die ISDN-Rufnummern reicht es im Prinzip aus, die letzten Stellen anzugeben, in denen sich die Rufnummern unterscheiden. Wenn Ihre Rufnummern (➤➤ **MSNs**) beispielsweise lauten: ***967310***, ***967311*** und ***967312***, brauchen Sie nur die ***10***, ***11*** und ***12*** berücksichtigen.

Lizenzkarte

Für die Grundkonfiguration brauchen Sie schließlich nur noch Ihre Lizenzkarte. Diese haben Sie zusammen mit **BinGO!** erhalten. Auf der Karte sind Seriennummer, Maske und Key angegeben, die Sie für eine Freischaltung der Funktionen von **BinGO!** benötigen. Auf der Lizenzkarte befindet sich auch die Lizenznummer für das Kommunikationsprogramm RVS-COM Lite.

Internetzugang

Wenn Sie einen Internetzugang einrichten wollen, brauchen Sie einen Internet Service Provider (kurz ISP). Daran haben Sie wahrscheinlich schon gedacht. Wenn nicht, sollten Sie das in den nächsten Tagen nachholen und dann mit der Konfiguration fortfahren. Von Ihrem ISP bekommen Sie Ihre persönlichen Zugangsdaten mitgeteilt. Die Bezeichnungen der benötigten Zugangsdaten können unter Umständen von ISP zu ISP leicht variieren. Grundsätzlich jedoch handelt es sich um die gleiche Art von Information, die Sie zur Einwahl und Festlegung Ihres persönlichen Internetzugangs benötigen. In der nachfolgenden Tabelle sind die Zugangsdaten zusammengestellt, die auch **BinGO!** für eine Verbindung zum Internet benötigt.

Zugangsdaten	Beispielswert	Ihre Werte
Providername	***GoInternet***	
Einwahlnummer Die Rufnummer, unter der Sie sich beim Internet Service Provider einwählen.	***1234567***	
Anschlußkennung Ihr Benutzername	***MyName***	
Paßwort	***TopSecret***	

Wenn **BinGO!** 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.

Einige Internet Service Provider wie z. B. T-Online brauchen zusätzlich Informationen:

Zugangsdaten	Beispielswert	Ihre Werte
T-Online-Nummer	***081512345678***	
Mitbenutzerkennung	***0001***	

Firmennetzanbindung

Für die Anbindung eines WAN-Partners (z. B. Firmenzentrale) müssen Sie einige Daten der Gegenstelle wissen, die Ihren Ruf annehmen soll. Genauso muß die Gegenstelle Daten von Ihnen wissen. Diese Daten müssen Sie gemeinsam absprechen.

Vor jeder Verbindung prüfen **BinGO!** und der Router Ihrer Firmenzentrale, ob sie den Ruf des Partners entgegennehmen. Die Rufannahme geschieht nur bei korrekter Authentisierung, um das Netz vor unbefugtem Zugriff zu schützen. Die Authentisierung erfolgt anhand des gemeinsamen Paßwortes und anhand von zwei Kennungen, die Sie und auch Ihr Partner für die Verbindung verwenden.

Zugangsdaten	Beispielswert	Ihre Wert
Partnername Kennung der Firmenzentrale	***BigBoss***	
Einwahlnummer Rufnummer des Routers der Firmenzentrale	***0911987654321***	
Lokaler Name Ihre eigene Kennung. Diesen Namen muß der Partner (Ihre Firmenzentrale) bei seinem Router als Partnernamen eintragen.	***LittleIndian***	
Paßwort Gemeinsames Paßwort für diese Verbindung	***Secret***	
Netzadresse(n) der Firmenzentrale	***10.1.1.0***	
Netzmaske(n) der Firmenzentrale	***255.255.255.0***	

Wie Sie weitere Sicherheitsmechanismen anwenden, z. B. Authentisierung anhand der Rufnummer (CLID) oder Verbergen des eigenen Netzes nach außen (NAT), erklärt Ihnen Kapitel 8, Seite 235.

Wenn **BinGO!** 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.

Netzadresse und Netzmaske des WAN-Partners (Firmenzentrale) brauchen Sie nur, wenn Sie zusätzlich zur LAN-LAN-Kopplung einen Internetzugang einrichten. Wenn Sie keinen Internetzugang einrichten, wird **BinGO!** so konfiguriert, daß automatisch alle Daten zum WAN-Partner geleitet werden, die nicht für das eigene Netz bestimmt sind (Default-Route).

3.2.2 Was in Ihrem Windows-Netzwerk zu tun ist

Nun haben Sie alle Daten gesammelt, die **BinGO!** wissen muß.

Damit aber alles richtig funktioniert, müssen Sie auch kontrollieren, ob Ihre Rechner im Netzwerk entsprechend konfiguriert sind. Wenn nicht, müssen Sie einige Einstellungen vornehmen.

Damit die Rechner in Ihren Netzwerk untereinander kommunizieren können, brauchen sie eine gemeinsame Verständigungsmethode. Das TCP/IP-Protokoll ist eine solche "Sprache", mit der die Rechner im LAN oder mit dem Internet ihre Informationen austauschen. Bevor Sie also mit der Konfiguration beginnen, stellen Sie sicher, daß dieses Protokoll installiert ist.

TCP/IP-Protokoll prüfen

Um zu prüfen, ob Sie das TCP/IP-Protokoll installiert haben, oder um TCP/IP jetzt zu installieren, gehen Sie folgendermaßen vor:

- Klicken Sie im Windows-Startmenü auf **Einstellungen** ➧ **Systemsteuerung**.
- Doppelklicken Sie auf **Netzwerk**.

Windows 95/98

- Suchen Sie in der Liste der Netzwerkkomponenten **TCP/IP**.
- Wenn Sie den Eintrag nicht finden, installieren Sie das TCP/IP-Protokoll wie unten beschrieben.

Windows NT

- Wählen Sie das Register **Protokolle** und suchen Sie in der Liste der Netzwerkkomponenten **TCP/IP-Protokoll**.
- Wenn Sie den Eintrag nicht finden, installieren Sie das TCP/IP-Protokoll wie unten beschrieben.

TCP/IP-Protokoll installieren

Windows 95/98

- Klicken Sie im Dialogfenster **Netzwerk** auf **Hinzufügen**.
- Wählen Sie in der Liste der Netzwerkkomponenten **Protokoll** und klicken Sie auf **Hinzufügen**.
- Wählen Sie als Hersteller **Microsoft** und als Netzwerkprotokoll **TCP/IP** und klicken Sie auf **OK**.

- Wenn Sie ein bestehendes Netzwerk haben, müssen Sie an dieser Stelle eventuell weitere Einstellungen vornehmen. Fragen Sie Ihren System-Administrator.
- Wenn Sie ein neues Netzwerk einrichten, klicken Sie auf **OK**.
- Folgen Sie den Anweisungen am Bildschirm und starten Sie zum Schluß den Rechner neu.
- Wiederholen Sie die Installation für alle Rechner im Netz.

Windows NT

- Klicken Sie im Dialogfenster **Netzwerk** auf das Register **Protokolle**. Klikken Sie auf **Hinzufügen**.
- Wählen Sie in der Liste der Netzwerkprotokolle **TCP/IP-Protokoll**. Klicken Sie auf **OK**.
- Wenn Sie ein neues Netzwerk einrichten, bestätigen Sie die Frage mit **Ja**.
- Bei einem bestehenden Netzwerk fragen Sie Ihren System-Administrator.
- Folgen Sie den Anweisungen am Bildschirm und starten Sie zum Schluß den Rechner neu.

Abschließend

- Wiederholen Sie die Installation für alle Rechner im Netz, wenn Sie dort LAN-LAN-Kopplung, Internetzugang oder Kommunikationsanwendungen über **BinGO!** nutzen wollen.

3.3 BRICKware unter Windows installieren

- Schließen Sie alle Windows-Programme auf Ihrem PC.
- Legen Sie Ihre BinTec Companion CD in das CD-ROM-Laufwerk Ihres PCs ein.

  Nach kurzer Zeit erscheint automatisch das Startfenster.
- Wenn das Startfenster nicht automatisch erscheint, klicken Sie im Windows Explorer auf Ihr CD-ROM-Laufwerk und doppelklicken Sie auf **setup.exe**.
- Klicken Sie im Startfenster auf **BRICKware**.

  Das Setup-Programm startet.
- Geben Sie das Verzeichnis an, in das BRICKware installiert werden soll.
- Klicken Sie auf **Next**.
- Wählen Sie Ihren Router aus, also **BinGO!**.
- Klicken Sie auf **Next**.
- Wählen Sie die Softwarekomponenten aus, die Sie installieren wollen. Sie können die eingestellte Auswahl übernehmen. In der Gruppe **Administration Tools** sollten Sie die Markierung des **Configuration Wizard** nicht aufheben, wenn Sie eine Grundkonfiguration von **BinGO!** mit dem Configuration Wizard durchführen wollen.
- Klicken Sie auf **Next**.

  Die Dateien werden kopiert. Nach kurzer Zeit erscheint ein Meldungsfenster, daß Ihre alte autoexec.bat gespeichert wird.
- Klicken Sie auf **OK**.

  Wenn Sie die DIME Tools installiert haben, erscheint ein Meldungsfenster, ob Sie die DIME Tools automatisch starten wollen.
- Sie können auf **Nein** klicken. Für die Grundkonfiguration von **BinGO!** ist dies nicht erforderlich.

  Es erscheint ein Fenster, in dem Sie wählen, wie Sie **BinGO!** konfigurieren wollen.

➤ Klicken Sie auf **Initial BRICK configuration with the Wizard** und anschließend auf **Next**.

Es erscheint ein Meldungsfenster, daß Sie den PC booten müssen, um den JAVA Statusmonitor zu verwenden.

➤ Klicken Sie auf OK.

Es erscheint ein Meldungsfenster, daß der Configuration Wizard gestartet wird.

➤ Klicken Sie auf OK.

Der Configuration Wizard startet.

3.4 BinGO! unter Windows konfigurieren

Im Kapitel 3.3, Seite 46 haben Sie den Configuration Wizard gestartet, mit dem Sie nun die Konfiguration von **BinGO!** durchführen.

Folgenden Konfigurationsschritte stehen zur Wahl:

- Router-Grundkonfiguration
- Internetzugang
- Firmennetzanbindung

Wenn Sie während der Konfiguration Fragen haben, steht Ihnen eine umfangreiche Online-Hilfe zur Verfügung. Um unsere kontext-sensitive Online-Hilfe aufzurufen:

➤ Drücken Sie **F1** oder klicken Sie auf **Hilfe**.

Wenn Sie eine bestehende Konfiguration bereits mit dem Configuration Wizard erstellt haben, dann kann der Wizard die Werte der bestehenden Konfiguration einlesen und übernehmen. Am Ende der Konfiguration überträgt der Wizard die neue Konfigurationsdatei zum Router und speichert sie zusätzlich auf Ihrem Rechner ab.

Die ursprüngliche Konfigurationsdatei von **BinGO!** können Sie außerdem am Ende der Konfiguration auf dem Router (unter old_cfg) sichern, sofern Sie das Paßwort dieser Konfiguration wissen.

Wenn Sie **BinGO!** direkt an einem Anlagenanschluß (Point-to-Point) betreiben, müssen Sie zusätzlich zu den Einstellungen des Configuration Wizard im Setup Tool eine Eintragung machen. Wählen Sie im Menü ***CM-1BRI, ISDN S0*** ➧ ***INCOMING CALL ANSWERING*** für den Ziffernvergleich der eingehenden Nummer den Modus *left to right (DDI)*. Der Wizard nimmt diese Einstellungen nicht automatisch vor, da dies nicht der Standardfall ist. Siehe dazu Kapitel 6.1.4, Seite 133.

Configuration Wizard starten

Wenn der Configuration Wizard noch nicht gestartet ist, gehen Sie folgendermaßen vor:

➤ Klicken Sie im Windows-Startmenü auf **Programme** ➧ **BRICKware** ➧ **Configuration Wizard**.

Das Startfenster des Configuration Wizard erscheint:

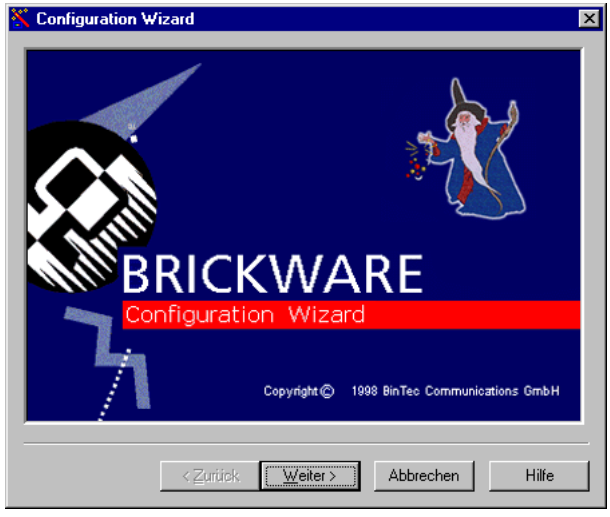


Bild 3-2: Startfester Configuration Wizard

➤ Klicken Sie auf **Weiter**.

Konfigurationsmodus einstellen

Im nächsten Fenster wählen Sie zwischen Quick- und Expert-Modus.

➤ Wenn Sie wenig Erfahrung mit Netzwerktechnologie haben, wählen Sie den Modus **Quick**. Im Folgenden erklären wir die Konfiguration anhand des Quick-Modus.

➤ Wenn Sie bereits Erfahrung mit Netzwerktechnologie und der Konfiguration von Routern haben, wählen Sie den Modus **Expert.**

So können Sie z. B.:

- Ihren Router als DHCP-Server einrichten.
- Unterschiedliche Benutzer für Kommunikationsanwendungen einrichten.
- Ihre ISDN-Rufnummern verschiedenen Diensten zuordnen (z. B. Fax).
- Umfangreichere Filter definieren.

➤ Klicken Sie auf **Weiter**.

Es erscheint ein Hinweis, daß der Router für eine serielle Verbindung neu gestartet werden muß.

Serielle Verbindung herstellen

➤ Klicken Sie auf **Weiter**.

Der Configuration Wizard stellt eine Verbindung zu **BinGO!** her. Der Router wird im Anschluß neu gestartet und der Typ des Routers erkannt: in Ihrem Fall **BinGO!**.

Wenn der Configuration Wizard keine Verbindung herstellen kann und eine Fehlermeldung erscheint:

➤ Prüfen Sie, ob Sie **BinGO!** richtig angeschlossen haben.

➤ Prüfen Sie, ob ein Terminalprogramm (z. B. Hyperterminal) oder ein anderes Programm gestartet ist, das die serielle Schnittstelle bereits belegt. Wenn ja, beenden Sie dieses Programm.

➤ Überlegen Sie, ob Sie die Baudrate bei **BinGO!** geändert haben. Im Auslieferungszustand sind 9600 bit/s eingestellt. Wenn Sie die Baudrate verändert haben, stellen Sie wieder 9600 bit/s ein.

➤ Wenn der Configuration Wizard **BinGO!** nicht booten konnte, schalten Sie **BinGO!** aus und wieder ein. Warten Sie, bis die LEDs nicht mehr blinken.

➤ Klicken Sie auf **Weiter**.

➤ Klicken Sie auf **OK** und dann auf **Weiter**.

Konfigurationspunkte auswählen

➤ Wählen Sie eine oder mehrere der folgenden Optionen:

– **Router-Grundkonfiguration**, um die grundlegenden Routereinstellungen vorzunehmen (Kapitel 3.4.1, Seite 51).

– **Internetanbindung**, um Ihren Internetzugang einzurichten (Kapitel 3.4.2, Seite 55).

– **Firmennetzanbindung**, um eine Firmennetzanbindung z. B. zu einer Firmenzentrale zu ermöglichen (Kapitel 3.4.3, Seite 56).

Die grundlegenden Routereinstellungen müssen Sie in jedem Fall vornehmen.

➤ Klicken Sie auf **Weiter**.

3.4.1 Router-Grundkonfiguration einrichten

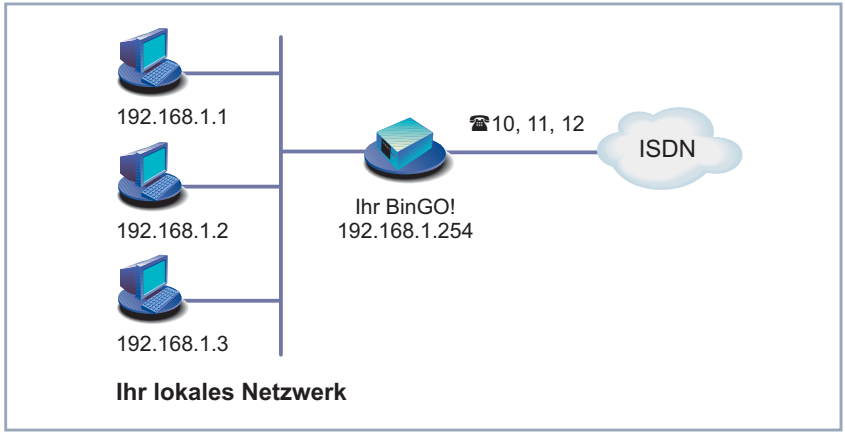


Bild 3-3: Grundkonfiguration von **BinGO!**

Achtung!

Alle BinTec-Router werden mit gleichem Benutzernamen und Paßwort ausgeliefert. Sie sind daher nicht gegen einen unauthorisierten Zugriff geschützt, solange Sie nicht das Paßwort geändert haben.

➤ Ändern sie daher unbedingt Ihr Systempaßwort, wenn Sie dazu aufgefordert werden.

➤ Geben Sie als erstes Ihre Lizenzdaten ein. Diese finden Sie auf Ihrer Lizenzkarte. Klicken Sie auf **Weiter**.

Der Configuration Wizard untersucht die Einstellungen des PCs, auf dem er gestartet ist und leitet daraus im Folgenden Vorschläge für die Konfiguration ab.

Unkonfiguriertes Netzwerk

➤ Wenn Ihr Rechner noch unkonfiguriert ist, noch keine IP-Adresse hat und als DHCP-Client eingerichtet ist, fragt Sie der Configuration Wizard, ob Sie **BinGO!** als DHCP-Server einrichten und die vorgeschlagenen Einstellungen beibehalten wollen.

➤ Klicken Sie auf **Weiter**.

BinGO! erhält die IP-Adresse ***192.168.1.254*** und vergibt an alle Rechner im Netzwerk automatisch IP-Adressen, beginnend bei ***192.168.1.1***.

Wenn Sie sich mit Netzwerktechnik auskennen, keinen DHCP-Server wollen oder die Einstellungen für DHCP-Server und IP-Adressen selbst vornehmen möchten:

- Deaktivieren Sie das Feld **Diesen Konfigurationsvorschlag übernehmen**.
- Geben Sie als nächstes die IP-Adresse für **BinGO!** und die zugehörige Netzmaske ein, z. B. ***192.168.1.254*** und ***255.255.255.0***. Klicken Sie auf **Weiter**.
- Geben Sie an, ob Sie **BinGO!** als DHCP-Server einrichten wollen. Wenn ja, geben Sie den IP-Adressbereich für Ihre PCs ein und bestimmen Sie die Anzahl der IP-Adressen, die von **BinGO!** vergeben werden.

Denken Sie daran, Ihren Rechnern im Anschluß an die Konfiguration feste IP-Adressen zu geben, falls Sie keinen DHCP-Server eingerichtet haben (vgl. Kapitel 3.6.1, Seite 63).

Bereits konfiguriertes Netzwerk

- Wenn Ihr Rechner eine feste IP-Adresse hat, fragt Sie der Configuration Wizard im Fenster **IP-Adresse des Routers im LAN** nach der IP-Adresse von **BinGO!** und der zugehörigen Netzmaske. Geben Sie die Werte ein, z. B. ***192.168.1.254*** und ***255.255.255.0***.
- Klicken Sie auf **Weiter**.
- Geben Sie ein neues Paßwort für Ihre Zugangsberechtigung ein.
- Klicken Sie auf **Weiter**.
  Alle Systempaßwörter sind mit diesem neuen Paßwort versehen.
- Geben Sie die Rufnummern Ihres ISDN-Anschlusses ein, die Sie mit **BinGO!** verwenden wollen: Geben Sie im Feld **Rufnummern** eine Rufnummer ein und klicken Sie auf **Hinzufügen**. Wiederholen Sie die Eingabe für alle weiteren Rufnummern. (Vgl. Bild 3-4, Seite 53)

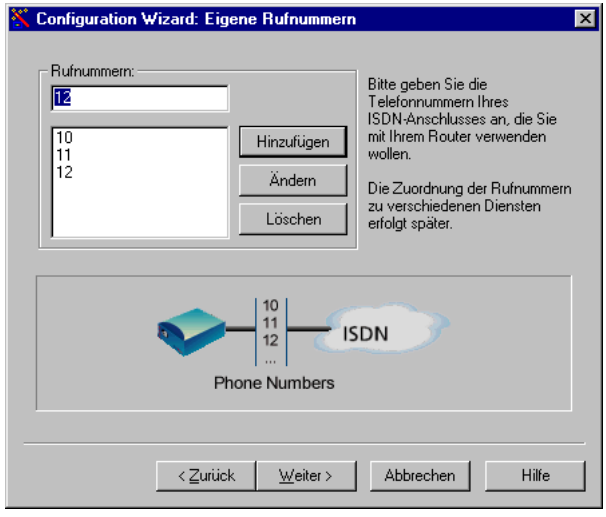


Bild 3-4: Rufnummerneingabe im Configuration Wizard

➤ Klicken Sie auf **Weiter**.

Der Configuration Wizard ordnet die Rufnummern automatisch bestimmten Diensten zu (mehr zu Diensten und Benutzern in Kapitel 4.3, Seite 84). Die Zuordnungen können Sie nur im Expert-Modus ändern. (Vgl. Bild 3-5, Seite 54)

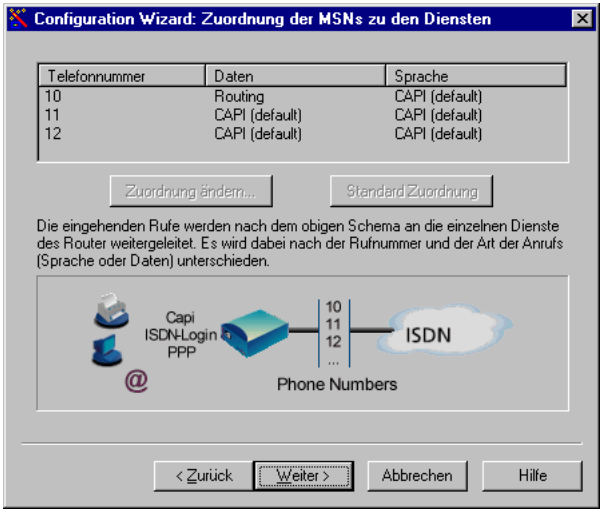


Bild 3-5: Rufnummernzuordnung im Configuration Wizard

➤ Klicken Sie auf **Weiter**.

Die Grundkonfiguration ist beendet. Es erscheint eine Zusammenfassung des letzten Punktes. Im Expert-Modus können Sie zusätzlich:

- Die Systemdaten ändern, z. B. Betreuer, Name und Standort von **BinGO!**
- Die IP-Adresse eines DNS-Servers angeben
- Die Systemzeit von anderer Stelle als vom ISDN beziehen lassen
- ISDN-Login erlauben
- Unterschiedliche Systempaßwörter setzen
- Kommunikationsanwendungen unterschiedlichen Benutzern und Rufnummern zuordnen
- Umfangreichere Filter setzten (NetBIOS, CAPI und TAPI Clients)
- Systemmeldungen protokollieren lassen

3.4.2 Mit BinGO! ins Internet

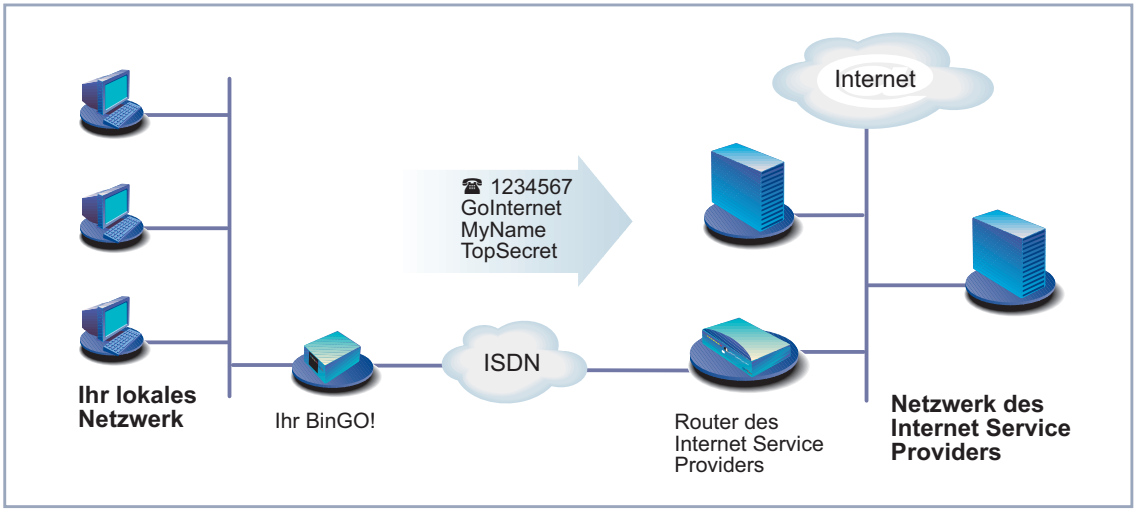


Bild 3-6: **BinGO!** und Ihr Internet Service Provider

- Klicken Sie auf **Weiter**.

  Es erscheint ein Informationsfenster.

- Wenn Sie die Informationen im Fenster gelesen haben, klicken Sie auf **Weiter**.

- Bestimmen Sie als erstes Ihren Internet Service Provider. Sie wählen zwischen:
  - Compuserve
  - T-Online
  - Spacenet
  - Einem anderen beliebigen Internet Service Provider

- Klicken Sie auf **Weiter**.

- Geben Sie den Namen des Internet Service Providers und die zugehörige Einwahlnummer ein, z. B. ***GoInternet*** und ***1234567***.

- Klicken Sie auf **Weiter**.

➤ Geben Sie Ihre Teilnehmerkennung (oft Benutzername) und das zugehörige Paßwort ein, z. B. ***MyName*** und ***TopSecret***.
Wenn Sie T-Online als Internet Service Provider gewählt haben, geben Sie T-Online-Nummer, Paßwort, Anschlußkennung (z. B. ***081512345678***) und Mitbenutzerkennung (z. B. ***0001***) ein.

➤ Klicken Sie auf **Weiter**.

Die Konfiguration Ihres Internetanschlusses ist beendet. Es erscheint eine Zusammenfassung des letzten Punktes. Im Expert-Modus können Sie zusätzlich:

- IP-Verbindungsdaten protokollieren lassen
- Komprimierung einschalten
- Den Zeitpunkt angeben, wann Gebühreninformationen vom ISDN bezogen werden und den Verbindungsabbau genauer festlegen (dynamischer und statischer Shorthold)

3.4.3 BinGO! ans Firmennetz anbinden

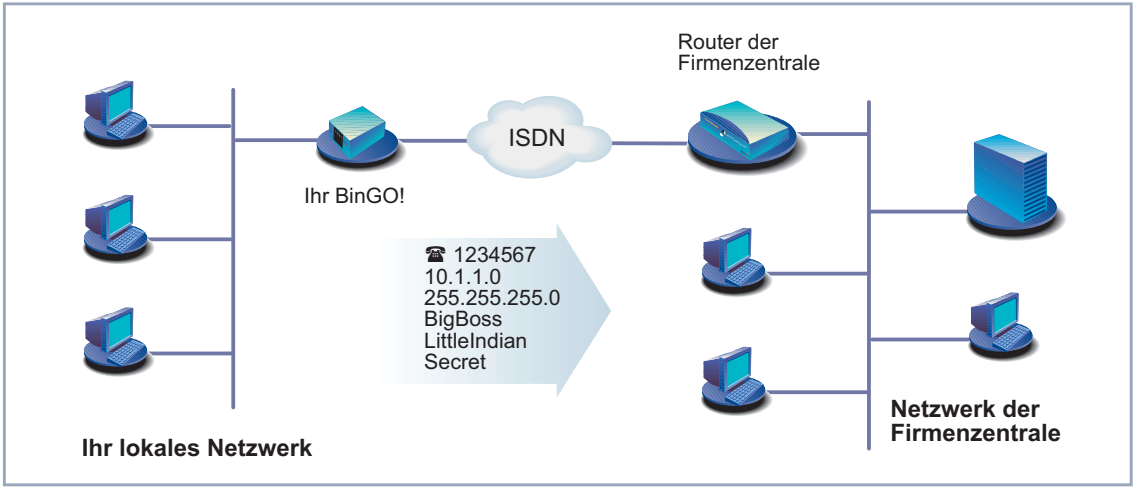


Bild 3-7: **BinGO!** und Ihre Firmenzentrale

➤ Klicken Sie auf **Weiter**.
Es erscheint ein Informationsfenster.

- Klicken Sie auf **Weiter**, nachdem Sie die Informationen im Fenster gelesen haben.
- Geben Sie als erstes den Namen Ihres WAN-Partners (z. B. der Firmenzentrale) und die zugehörige Einwahlnummer ein, z. B. ***BigBoss*** und ***0911987654321***.
  Der Name des WAN-Partners muß mit dem Namen übereinstimmen, den Ihr Partner als lokalen Namen verwendet. Ihr Partner muß Anrufe auf die angegebene Einwahlnummer mit dem Dienst Routing annehmen.
- Klicken Sie auf **Weiter**.
- Geben Sie Ihren lokalen Namen und das gemeinsame Paßwort ein, z. B. ***LittleIndian*** und ***Secret***.
  Ihr lokaler Name muß mit dem Namen übereinstimmen, den ihr Partner für Sie als WAN-Partner verwendet.
- Klicken Sie auf **Weiter**.
- Fügen Sie eine Route zu Ihrer Firmenzentrale hinzu:
  Wenn Sie keinen Internetzugang eingerichtet haben, dann wählen Sie **Default Route verwenden**.
  Wenn Sie einen Internetzugang eingerichtet haben, dann geben Sie selbst die Route ein: Klicken Sie auf **Hinzufügen**. Geben Sie die IP-Adresse oder Netzadresse und die Netzmaske ein, z. B. ***10.1.1.0*** und ***255.255.255.0***. Anhand der Route legen Sie die Verbindung zu Ihrem WAN-Partner (z. B. Firmenzentrale) fest. (Vgl. Bild 3-8, Seite 58)

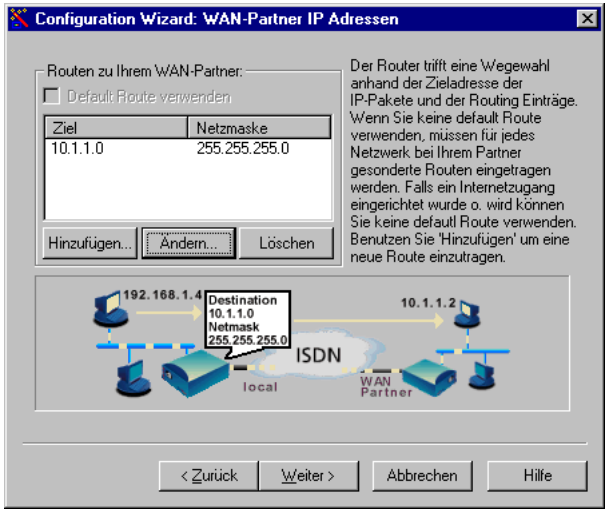


Bild 3-8: Route zum WAN-Partner im Configuration Wizard festlegen

Jede Route bestimmt den Weg zu einem Netz oder Teilnetz bei Ihrem WAN-Partner. Eine Route ist durch IP-Adresse/Netzadresse und Netzmaske eindeutig festgelegt.

Statt der Netzadresse können Sie auch eine beliebige IP-Adresse aus dem Partnernetz eingeben. Anhand der zugehörigen Netzmaske ermittelt der Configuration Wizard automatisch die Netzadresse.

- Klicken Sie auf **OK**.
- Wenn Ihre Zentrale ein Netzwerk aus mehreren Einzelnetzen betreibt, und Sie in jedes dieser Einzelnetze gelangen wollen, dann geben Sie für jedes weitere Einzelnetz eine Route ein (vgl. Bild 4-3, Seite 95).
- Klicken Sie auf **Weiter**.

Die Konfiguration Ihres WAN-Partners ist beendet. Es erscheint eine Zusammenfassung des letzten Punktes. Im Expert-Modus können Sie zusätzlich:

- Eine automatische Rückruffunktion einrichten, damit nur einer der beiden Partner die Telefongebühren übernimmt
- Die Rufnummer des Anrufers prüfen: Calling Line Identification (CLID)

- IP-Verbindungsdaten protokollieren lassen
- Back Route Verify aktivieren, um die Einspeisung von manipulierten Datenpaketen zu verhindern
- Komprimierung, Verschlüsselung und Kanalbündelung definieren
- Den Zeitpunkt angeben, wann Gebühreninformationen vom ISDN bezogen werden und den Verbindungsabbau genauer festlegen (dynamischer und statischer Shorthold)

3.4.4 Konfiguration abschließen

➤ Klicken Sie auf **Weiter**.

➤ Wählen Sie **Bestehende Konfiguration auf dem Router sichern**, um eine bereits vorhandene Konfiguration vor Überschreiben zu sichern.

➤ Klicken Sie auf **Fertigstellen**, um die Konfiguration abzuschließen.

Der Configuration Wizard loggt sich auf **BinGO!** ein. Eine bestehende Konfiguration wird als old_cfg auf dem Router gesichert. Die neu erstellte Konfiguration wird zu **BinGO!** übertragen und zusätzlich auf Ihrem Rechner unter dem Namen brick.cfg im Installationsverzeichnis BRICK gespeichert. Nach einiger Zeit erscheint eine Meldung, daß die Konfiguration abgeschlossen ist.

Falls eine Fehlermeldung erscheint, daß der Configuration Wizard sich nicht auf dem Router einloggen konnte, weil das Passwort geändert ist:

➤ Wenn Sie das Passwort der bestehenden Konfiguration wissen, geben Sie das Passwort ein und klicken Sie auf **OK**.

Der Configuration Wizard versucht, sich auf **BinGO!** einzuloggen.

➤ Falls dies scheitert, können Sie die Eingabe mehrmals wiederholen oder auf **nicht bekannt** klicken. Wenn Sie auf **nicht bekannt** klicken, wird die alte Konfiguration überschrieben, die neue auf dem Router gesichert.

➤ Wenn Sie das Passwort nicht wissen, klicken Sie auf **nicht bekannt** und anschließend auf **OK**.

Die alte Konfiguration wird überschrieben, die neue auf dem Router gesichert.

Der Configuration Wizard sichert in jedem Fall Ihre neu erstellte Konfiguration auf dem PC, auch wenn Fehler bei der Übertragung zum Router auftreten.

Die auf dem PC gesicherte Konfigurationsdatei steht für weitere Einstellungen mit dem Wizard zur Verfügung.

➤ Klicken Sie auf **OK**.

Wenn Sie **BinGO!** als DHCP-Server und Ihre Rechner als DHCP-Clients eingerichtet haben (Standardfall), dann weist **BinGO!** den PCs jetzt die IP-Adressen zu. Unter Windows NT (Programm IPCONFIG) geschieht dies automatisch, unter Windows 95 (Programm WINIPCFG) müssen Sie die Zuweisung bestätigen.

➤ Klicken Sie **Ja**, um WINIPCFG zu starten. Klicken Sie auf **Aktualisieren** und dann auf **OK**.

Es erscheint eine Meldung, ob Sie den CAPI/TAPI-Server installieren wollen.

➤ Klicken Sie auf **Ja**.

Das Fenster Remote Clients Configuration erscheint:

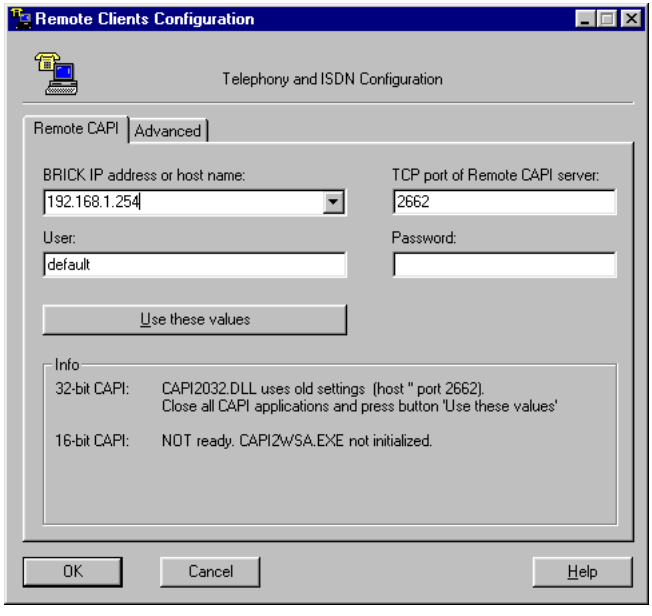


Bild 3-9: Remote-CAPI-Konfiguration

3.5 Remote-CAPI-Schnittstelle konfigurieren

Im Remote-CAPI-Konfigurationsprogramm tragen Sie **BinGO!** als CAPI-Server ein.

Der CAPI-Server von **BinGO!** ermöglicht:

- Auf jedem PC im Netzwerk Kommunikationsanwendungen zu betreiben (z. B. Faxdienste mit RVS-COM Lite)
- Gleichzeitig von mehreren PCs aus über Kommunikationsanwendungen auf das ISDN zuzugreifen

Um CAPI-Anwendungen auf jedem PC im Netzwerk zu ermöglichen, müssen Sie auf allen PCs die Remote-CAPI-Schnittstelle einrichten.

Auf dem ersten PC haben Sie bereits BRICKware installiert und das Konfigurationsfenster für die Remote-CAPI-Konfiguration erhalten (vgl. Bild 3-9, Seite 60). Sie können gleich mit Kapitel 3.5.2, Seite 62 fortfahren. Für alle weiteren PCs im Netz müssen Sie zunächst das Programm CAPI Configuration installieren wie in Kapitel 3.5.1, Seite 61 beschrieben.

3.5.1 Programm CAPI Configuration installieren

➤ Wenn noch nicht geschehen, installieren Sie die BRICKware wie im Kapitel 3.3, Seite 46 beschrieben, bis das Auswahlfenster **Configure your BRICK and this PC** erscheint.

➤ Im Auswahlfenster **Configure your BRICK and this PC** klicken Sie auf **Keep old BRICK configuration**.

➤ Klicken Sie auf **Next**.

Das Remote-CAPI-Konfigurationsfenster erscheint (vgl. Bild 3-9, Seite 60).

3.5.2 Remote-CAPI konfigurieren

- Geben Sie im Register **Remote CAPI** die IP-Adresse von **BinGO!** ein, z. B. ***192.168.1.254***.
- Wenn Sie den Quick-Modus im Configuration Wizard verwendet haben, behalten Sie im Feld **User** den Eintrag **default** bei.
- Wenn Sie im Expert-Modus des Configuration Wizard mehrere Benutzer eingerichtet haben, dann geben Sie den Benutzernamen und ein Paßwort ein. Die Rechte, die Sie während der Konfiguration für diesen Benutzer festgelegt haben, sind damit am aktuellen PC gültig.
- Klicken Sie auf **Use these values**.

  Nach kurzer Zeit erscheint eine Meldung "Remote CAPI is ready".

Wenn nach Klicken auf **Use these values** eine Fehlermeldung erscheint, prüfen Sie, ob

- die IP-Adresse von **BinGO!** stimmt.
- Sie einen gültigen Benutzer eingegeben haben.
- die richtige Port-Nummer 2662 eingetragen ist.
- Ihr Rechner als DHCP-Client konfiguriert ist und vielleicht noch keine IP-Adresse bekommen hat (siehe Kapitel 4.4, Seite 88).

- Wenn keine Fehlermeldung erscheint, klicken Sie auf **OK**.
- Wiederholen Sie die Remote-CAPI-Installation auf allen PCs im Netz, auf denen Sie Kommunikationsanwendungen (z. B. Fax) ermöglichen wollen.

Genauere Beschreibungen zur Remote-CAPI-Konfiguration finden Sie in BRICKware for Windows. Dort ist auch die Multibrick-CAPI für Windows NT beschrieben, mit der Sie mehre BRICKs im Netzwerk als CAPI-Server definieren.

3.6 PC einrichten

Damit Ihr Netzwerk und die Verbindung nach draußen richtig funktionieren, müssen Sie unter Umständen zusätzliche Einstellungen an Ihren Rechnern vornehmen:

- Wenn Sie mit dem Configuration Wizard **BinGO!** nicht als DHCP-Server eingerichtet und die Rechner bisher keine IP-Adressen haben, müssen Sie (gemäß Kapitel 3.6.1, Seite 63):
  - die IP-Adressen jetzt festlegen
  - den Rechnern den "Weg nach draußen" (Gateway, DNS-Server) zeigen

  Falls Sie die Standardeinstellungen des Configuration Wizard übernommen haben und Sie Ihre PCs als DHCP-Clients eingerichtet haben, brauchen Sie das Kapitel Kapitel 3.6.1, Seite 63 nicht berücksichtigen. **BinGO!** liefert in diesem Fall die nötigen Informationen automatisch.
- Wenn Sie eine Firmennetzanbindung konfiguriert haben, wollen Sie sicherlich Rechner aus dem Partner-LAN (z. B. Firmenzentrale) über Ihr Windows erreichen. Dazu müssen Sie vorgehen, wie in Kapitel 3.6.2, Seite 64 beschrieben.

3.6.1 Dem Rechner IP-Adresse, Gateway und DNS-Server mitteilen

Falls Sie **BinGO!** nicht als DHCP-Server eingerichtet und Ihre Rechner noch keine IP-Adressen haben, müssen Sie den Rechnern jetzt sagen, unter welcher IP-Adresse sie erreichbar sein sollen. Zusätzlich müssen Sie den Rechnern mitteilen, wo der "Weg nach draußen", z. B. ins Internet führt. Gehen Sie folgendermaßen vor:

➤ Klicken Sie im Windows-Startmenü auf **Einstellungen** ➧ **Systemsteuerung**.

➤ Doppelklicken Sie auf **Netzwerk**.

Windows 95/98

➤ Klicken Sie auf **TCP/IP** ➧ **Eigenschaften**.

- Geben Sie im Register **IP-Adresse** eine eindeutige IP-Adresse für Ihren Rechner und die Netzmaske ein, z. B. ***192.168.1.1*** und ***255.255.255.0.***
- Geben Sie im Register **Gateway** die IP-Adresse von **BinGO!** ein, z. B. ***192.168.1.254***. Klicken Sie auf **Hinzufügen**.
- Wenn Sie keinen eigenen DNS-Server haben, geben Sie im Register **DNS-Konfiguration** unter **Suchreihenfolge für DNS-Server** die IP-Adresse von **BinGO!** ein, z. B. ***192.168.1.254***.

Windows NT

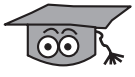
- Wählen Sie das Register **Protokolle**. Klicken Sie auf **TCP/IP-Protokoll** ➧ **Eigenschaften**.
- Klicken Sie im Register **IP-Adresse** auf **IP-Adresse angeben** und bestimmen Sie IP-Adresse, Netzmaske und Standard-Gateway, z. B. ***192.168.1.254***, ***255.255.255.0*** und ***192.168.1.1***. Als Standard-Gateway tragen Sie die IP-Adresse von **BinGO!** ein.
- Klicken Sie im Register **DNS** unter **Suchreihenfolge des DNS-Dienstes** auf **Hinzufügen** und geben Sie die IP-Adresse von **BinGO!** ein, z. B. ***192.168.1.254***.

Zum Schluß

- Bestätigen Sie alle Eingaben und starten Sie zum Schluß den Rechner neu.
- Wiederholen Sie die Installation für alle Rechner im Netz.

3.6.2 Die Rechner des Partnernetzes finden

Sie haben jetzt bei **BinGO!** alles für eine Verbindung zu Ihrem Partnernetz eingestellt. Nun wollen Sie beispielsweise von Ihrem PC aus auf den Windows-Rechner ***BossPC*** im Partnernetz zugreifen.



Dabei ist einiges zu beachten. Jeder Rechner in Ihrem LAN oder im Netzwerk Ihres Partners benötigt eine eindeutige Adresse, die IP-Adresse. In der Vergangenheit haben sich außer IP-Adressen auch sogenannte Computer- und Host-Namen entwickelt, um Rechner über deren Namen (wie z. B. ***BossPC***) anzusprechen. Die Computer-Namen werden speziell in Windows-Netzwerken verwendet. Rechner verstehen aber nur IP-Adressen und keine Namen. Daher muß es eine Stelle geben, welche die zu den Namen gehörigen IP-Adressen bekannt gibt – eine Namensauflösung durchführt (vgl. Kapitel 4.5, Seite 91). Typische Beispiele für eine solche Namensauflösung sind ein DNS- oder ein

WINS-Server. Da Sie in einem kleinen Netzwerk meist keinen eigenen Server einrichten wollen, gibt es eine andere Möglichkeit, wie Sie den Namen von ***BossPC*** in eine IP-Adresse auflösen können: die LMHOSTS-Datei.

In der LMHOSTS-Datei ordnen Sie tabellarisch IP-Adressen den verschiedenen Computer-Namen zu. Wenn Sie dann nach dem Rechner ***BossPC*** suchen, der sich im Partnernetz (z. B. Firmenzentrale) befindet, fragt Ihr Rechner seine LMHOSTS-Datei nach der zugehörigen IP-Adresse und kann so den Rechner finden.

Achtung!

Bei der nachfolgend beschriebenen Konfiguration kann es zu erhöhten Verbindungsaufbauten und somit hohen Telefongebühren kommen. Die Bedingungen, die zum Verbindungsaufbau führen, hängen stark von der jeweiligen Netzwerk-Konfiguration ab. Speziell wenn Sie ein Netzlaufwerk verbinden, müssen Sie damit rechnen, daß regelmäßige Anfragen die Verbindungsaufbauten erhöhen.

➤ Um ungewollte Gebühren zu vermeiden, sollten Sie **BinGO!** unbedingt überwachen.

Das nachfolgend beschriebene Verfahren können Sie nur anwenden, wenn Sie mit dem Configuration Wizard im Expert-Modus keine umfangreiche NetBIOS-Filterung eingestellt haben. Sonst können bestimmte Windows-Funktionen wie z. B. eine Netzlaufwerksverbindung nicht genutzt werden.

Wenn Sie Zugang zum Partnernetz für mehrere Rechner in Ihrem Netz benötigen, müssen Sie die Zuordnung IP-Adresse zu Name auf allen diesen Rechnern abspeichern.

Außerdem sollten Sie beachten,

- daß Ihr WAN-Partner und Sie selbst in der gleichen Domäne oder Arbeitsgruppe sind.
- daß Sie von Ihrem WAN-Partner die erforderlichen Freigaben für Zugriffe auf Rechner des Partnernetzes erhalten. Fragen Sie im Zweifelsfall den Systemadministrator.

Sie können sich auch komplett an der Windows-NT-Domäne eines Partnernetzes anmelden. Um eine solche Konfiguration zu testen, stellt BinTec für Sie einen Testzugang bereit. Wie Sie diesen Zugang einrichten, erfahren Sie unter www.bintec.de im Abschnitt FAQ, Kategorie: BRICK/Testzugang "Router – Router".

Teilen Sie Ihrem PC die IP-Adresse des Rechners ***BossPC*** wie nachfolgend beschrieben mit, indem Sie die LMHOSTS-Textdatei bearbeiten:

- Klicken Sie im Windows-Startmenü auf **Suchen** ➧ **Dateien/Ordner...**.
- Geben Sie `lmhosts.*` ein.
- Klicken Sie auf **Starten**.
- Öffnen Sie die gefundene Datei mit einem Text-Editor.
- Tragen Sie IP-Adresse des Rechners im Partnernetz, gefolgt von einem Tabulator oder Leerzeichen, gefolgt von dem Namen des Rechners ein, z. B. `10.1.1.1 BossPC`. Speichern und schließen Sie die Datei unter dem Namen lmhosts.
- Gehen Sie für jeden weiteren Rechner des Partnernetzes, den Sie über Windows erreichen wollen, in gleicher Weise vor.
- Klicken Sie im Windows-Startmenü auf **Suchen** ➧ **Computer...**.
- Geben Sie den Namen des Rechners ein, z. B. ***BossPC*** und klicken Sie auf **Starten**.

  Nach kurzer Zeit erscheint der Rechnername.

Verknüpfung auf dem Desktop

- Damit Sie den Rechner nicht bei jedem Neustart des Rechners erneut suchen müssen, rechtsklicken Sie auf das Rechner-Symbol und klicken Sie auf **Verknüpfung herstellen**.

  Es erscheint die Frage, ob Sie eine Verknüpfung auf dem Desktop erstellen wollen.
- Klicken Sie auf **Ja**.

  Sie können jetzt jederzeit über Windows auf den Rechner ***BossPC*** des Partnernetzes zugreifen.

Netzlaufwerk verbinden

Alternativ können Sie eine Netzlaufwerkverbindung herstellen:

- Öffnen Sie den Windows-Explorer und klicken Sie unter **Extras** auf **Netzlaufwerk verbinden**.
- Bestimmen die Laufwerksbezeichnung und geben Sie den Pfad an, z. B. ***\\BossPC***.
- Klicken Sie auf **Verbindung beim Start wiederherstellen**.
- Klicken Sie auf **OK**.

3.7 Fax und Anrufbeantworter einrichten mit RVS-COM Lite

Faxen machen. Aber wie?

Nachdem Sie Rechner und **BinGO!** erfolgreich konfiguriert haben, installieren Sie RVS-COM Lite. Mit RVS-COM Lite können Sie:

- Faxe verschicken und empfangen
- Einen Anrufbeantworter einrichten
- Dateitransferdienste und Euro-Filetransferdienste einrichten

In den nachfolgenden Abschnitten beschreiben wir, wie Sie Ihrem Rechner und **BinGO!** das Faxen mit RVS-COM Lite (Version 1.56) beibringen und eine Anrufbeantworterfunktion einrichten.

Mit **BinGO!** haben Sie genau eine Lizenz für RVS-COM Lite.erhalten. Falls Sie RVS-COM Lite auf mehreren Rechnern installieren wollen, wenden Sie sich bitte an RVS Datentechnik GmbH. Die Anschrift können Sie der Online-Hilfe von RVS-COM Lite entnehmen.

3.7.1 RVS-COM Lite installieren

➤ Legen Sie Ihre BinTec Companion CD erneut in das CD-ROM-Laufwerk Ihres PCs ein.

Nach kurzer Zeit erscheint automatisch das Startfenster.

➤ Wenn das Startfenster nicht automatisch erscheint, klicken Sie im Windows Explorer auf Ihr CD-ROM-Laufwerk und doppelklicken Sie auf **setup.exe**.

➤ Klicken Sie im Startfenster auf **RVS-COM Lite**.

Das Setup-Programm startet.

➤ Geben Sie Ihre RVS-COM-Lizenznummer ein. Die Nummer befindet sich auf Ihrer Lizenzkarte.

➤ Klicken Sie auf **Installieren**.

Das Startfenster erscheint.

- Bestätigen Sie die beiden folgenden Fenster und geben Sie das Verzeichnis an, in das RVS-COM Lite installiert werden soll. Klicken Sie auf **Weiter**.

  Die Dateien werden kopiert. Nach kurzer Zeit erscheint ein Hinweis, daß das Setup-Programm beendet ist.

- Klicken Sie auf **Beenden**.

  Das Startfenster des Installations-Assistenten erscheint:

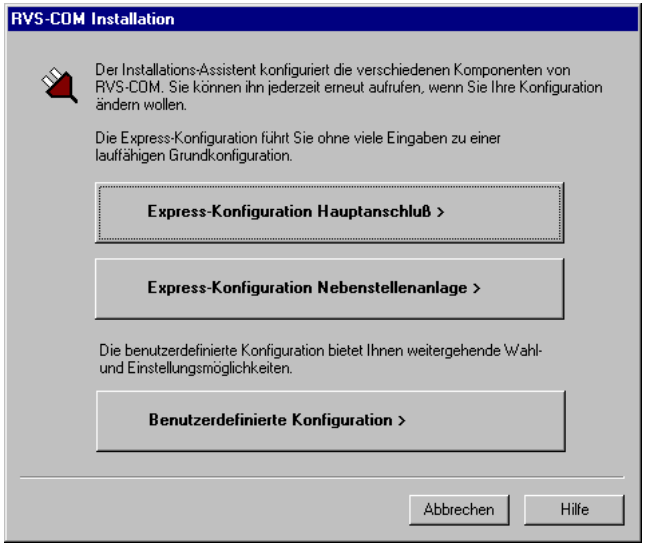


Bild 3-10: Startfenster des Installations-Assistenten von RVS-COM Lite

Falls eine Fehlermeldung erscheint, daß keine CAPI-Schnittstelle installiert ist:

- Prüfen Sie, ob Sie **BinGO!** mit Ihrem ISDN-Anschluß verbunden haben.
- Prüfen Sie, ob Ihre Remote-CAPI-Konfiguration eingerichtet ist, wie in Kapitel Kapitel 3.5.2, Seite 62 beschrieben.

Um empfangene Faxe mit einem Windows-E-Mail-System anstatt mit der RVS Inbox zu verwalten oder um RVS ISDN-Modems zu installieren (auch für das DFÜ-Netzwerk), wählen Sie den Konfigurations-Modus **Benutzerdefinierte Konfiguration**.

- Wenn **BinGO!** an einem Hauptanschluß (z. B. NTBA-Adapter) angeschlossen ist, klicken Sie auf **Express-Konfiguration Hauptanschluß**.
- Wenn **BinGO!** an einer TK-Anlage angeschlossen ist, klicken Sie auf **Express-Konfiguration Nebenstellenanlage**.
- Klicken Sie auf **Weiter**.

  Es erscheint ein Hinweis, daß Sie RVS-COM für den Betrieb mit einem ISDN-Adapter mit CAPI-Schnittstelle konfiguriert haben.
- Klicken Sie auf **Weiter**.
- Wenn ein Hinweis erscheint, daß Sie Wahlparameter (z. B. Amts- oder Ortskennzahl) ändern sollten, bestätigen Sie die Meldung, um Ihre Wahlparameter richtig einzustellen. Passen Sie die Einstellungen an. (Vgl. Bild 3-11, Seite 70)

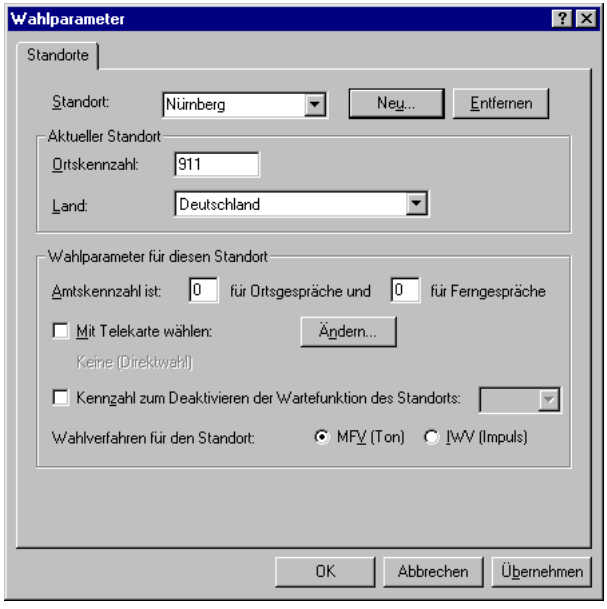


Bild 3-11: Wahlparameter

Die Ortskennzahl muß ohne führende "0" angegeben sein.

Die Amtskennzahlen brauchen Sie nur, wenn Sie **BinGO!** an einer TK-Anlage betreiben. Meist stimmen hier die Amtskennzahlen für Orts- und Ferngespräche überein (siehe Bild 3-11, Seite 70).

- Wenn Sie die Einstellungen angepaßt haben, klicken Sie auf **Übernehmen** und dann auf **OK**.
- Wenn Sie eine **Express-Konfiguration Hauptanschluß** durchführen, geben Sie im nächsten Fenster die Rufnummer Ihres ISDN-Anschlusses ein. Wählen Sie eine der Rufnummern, die Sie bereits im Configuration Wizard eingegeben haben. Mit dem Installations-Assistenten können Sie nur eine Rufnummer eingeben. Später können Sie weitere Rufnummern hinzufügen.
- Wenn Sie eine **Express-Konfiguration Nebenstellenanlage** durchführen, geben Sie in den beiden nächsten Fenstern Nebenstellennummer (von der TK-Anlage gemeldete Nummer) und Rufnummer beim Mehrgeräteanschluß bzw. Rufnummer und Durchwahl der Nebenstelle beim Anlagenanschluß ein.

Wenn Sie **BinGO!** direkt an einem Anlagenanschluß (Point-to-Point) betreiben, müssen zusätzlich zu den Einstellungen des Configuration Wizard im Setup Tool eine Eintragung machen. Wählen Sie im Menü ***CM-1BRI, ISDN S0*** ➧ ***INCOMING CALL ANSWERING*** für den Ziffernvergleich der eingehenden Nummer den Modus *left to right (DDI)*. Der Configuration Wizard nimmt diese Einstellungen nicht automatisch vor, da dies nicht der Standardfall ist. Siehe dazu Kapitel 6.1.4, Seite 133

- Klicken Sie auf **Weiter**.
- Klicken Sie in den folgenden Fenstern auf **Weiter** und schließlich auf **Beenden**.

  Die Konfiguration mit dem Installations-Assistenten ist abgeschlossen.

3.7.2 RVS-COM Lite einrichten

Im Folgenden müssen die Nummern, die Sie auch mit dem Configuration Wizard festgelegt haben, den verschiedenen Diensten (Fax, Anrufbeantworter) zu-

gewiesen werden. Das nachfolgende Bild verdeutlicht, welche Nummer in unserem Konfigurationsbeispiel für welche Funktion verwendet werden soll.

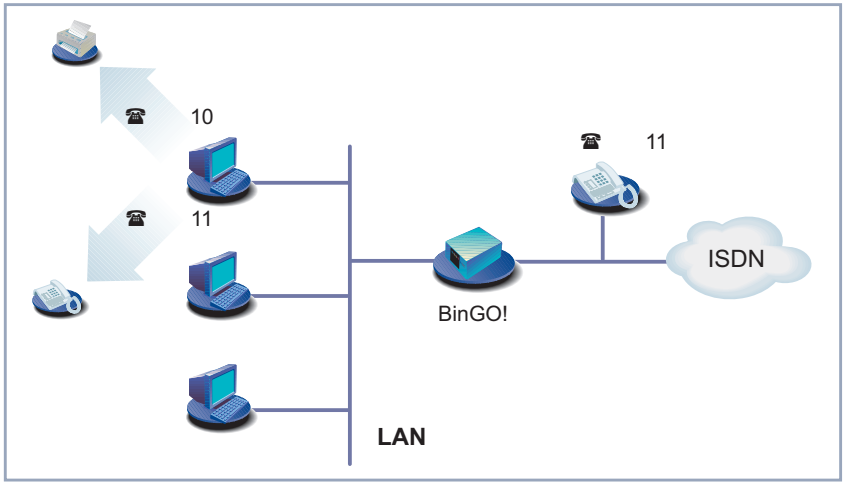


Bild 3-12: Szenario: 1 Telefon, 1 Rechner mit Fax und Anrufbeantworter

Dabei gehen wir davon aus, daß auf eine der Nummern (im Beispiel ***11***), die Sie im Configuration Wizard eingegeben haben, auch ein Telefon reagiert.

- Klicken Sie im Windows-Startmenü auf **Programme** ➧ **RVS-COM Lite** ➧ **CommCenter**.
- Klicken Sie im Register **Rufnummern** auf **Hinzufügen**, um weitere Rufnummern einzugeben. Geben Sie die Nummern ein, die Sie bereits bei der Router-Konfiguration mit dem Configuration Wizard verwendet haben (vgl. Bild 3-13, Seite 73).

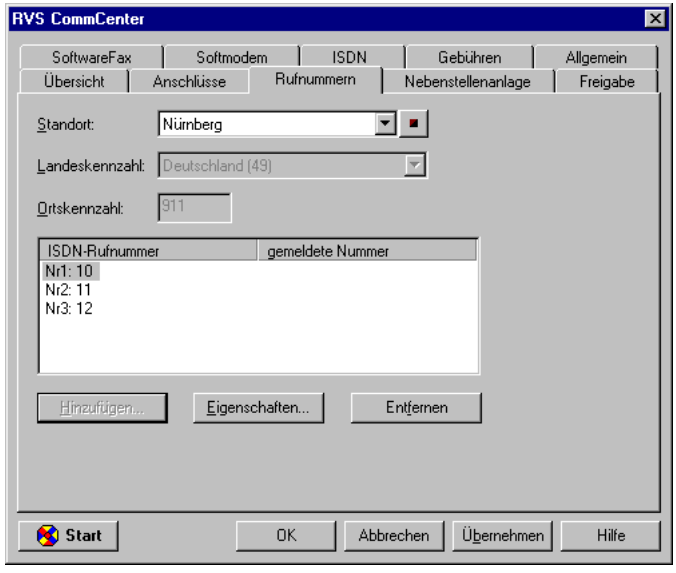


Bild 3-13: Rufnummernkonfiguration in RVS-COM Lite

- Wenn Sie alle Rufnummern eingegeben haben, klicken Sie auf **Übernehmen**.
- Klicken Sie im Register **Anschlüsse** auf **Eigenschaften**, um die Rufnummern den unterschiedlichen Diensten zuzuweisen (vgl. Bild 3-14, Seite 74).

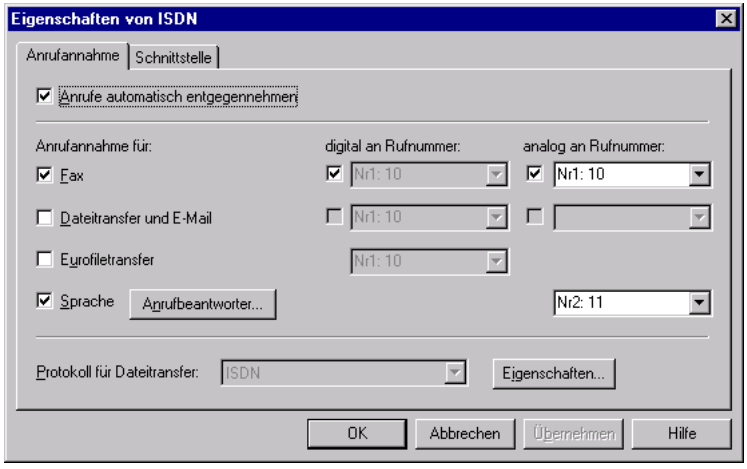


Bild 3-14: Zuordnung der Rufnummern auf Dienste in RVS-COM Lite

- Ordnen Sie die erste Rufnummer dem Dienst Fax zu, die zweite Rufnummer dem Dienst Sprache (Anrufbeantworter). Verwenden Sie unterschiedliche Rufnummern.
- Lassen Sie die anderen Dienste (Dateitransfer und Euro-Filetransfer) frei.
- Um die Anrufbeantworterfunktion anzupassen, klicken Sie auf **Anrufbeantworter** und ändern Sie ggf. Ansagetext und Anzahl der Klingelzeichen vor Rufannahme.
- Klicken Sie auf **OK**.
- Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

  In der Liste der Anschlüsse erscheint die Meldung "ISDN: Warten auf Anruf". CommCenter ist bereit, Anrufe und Faxe entgegenzunehmen.

3.8 Konfiguration testen

Sie haben es geschafft! Testen Sie nun, ob Sie alle Konfigurationseinstellungen richtig vorgenommen haben.

3.8.1 Internetzugang testen

➤ Konfigurieren Sie Ihren Browser, falls Sie dies noch nicht getan haben. Wenn Sie von Ihrem Internet Service Provider die IP-Adresse eines Proxy-Servers erhalten haben, können Sie IP-Adresse des Proxy-Servers eintragen. Achten Sie darauf, daß Sie eine Verbindung über Ihr lokales Netzwerk einrichten (vgl. Bild 3-15, Seite 75).

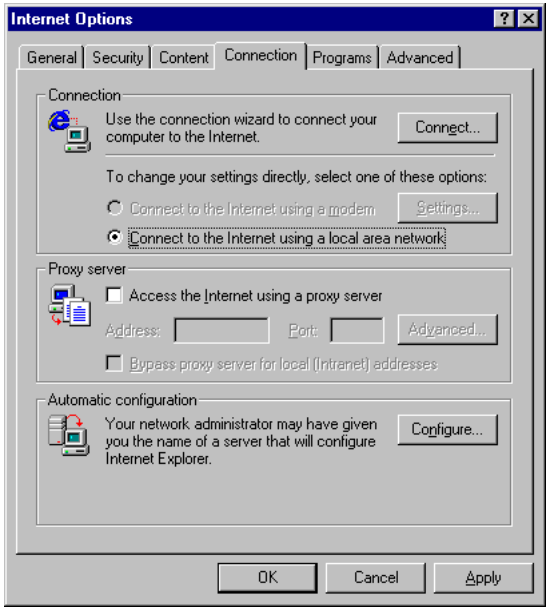


Bild 3-15: Browser-Konfiguration für Internetanbindung (Beispiel Internet Explorer)

➤ Geben Sie in Ihrem Browser www.bintec.de ein.

Die Homepage von BinTec Communications AG erscheint.

3.8.2 E-Mails verschicken und empfangen

- Legen Sie im E-Mail-Programm einen "Account" an, falls Sie noch keinen haben. Die Server für Incoming und Outgoing Mail haben Sie von Ihrem Internet Service Provider erhalten. Achten Sie darauf, daß Sie eine Verbindung über Ihr lokales Netzwerk einrichten (vgl. Bild 3-16, Seite 76).

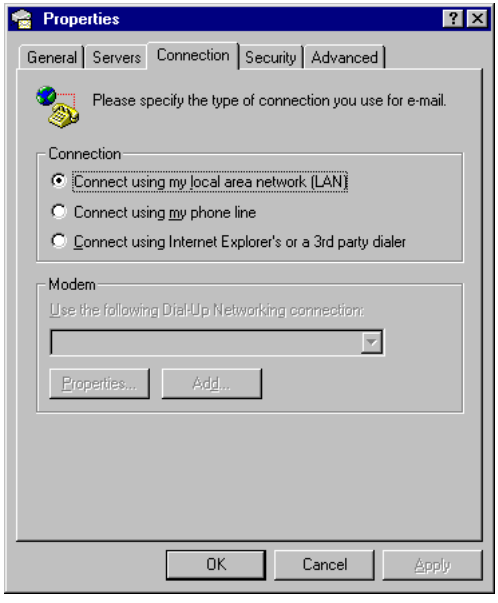


Bild 3-16: Konfiguration des E-Mail-Programms (Beispiel Microsoft Outlook Express)

- Schicken Sie eine E-Mail an einen guten Bekannten oder – wenn Sie wollen – direkt an BinTec! Verwenden Sie dazu die E-Mail-Adresse testmail@bintec.de und geben Sie als Betreff Testmail ein.

  Sie erhalten von uns umgehend eine Rückantwort, damit Sie kontrollieren können, ob alles geklappt hat.

3.8.3 Ein Fax verschicken

Schicken ein Test-Fax an einen guten Bekannten oder schicken Sie das Test-Fax an sich selbst – indem Sie für die Rufnummer des Empfängers Ihre eigene neue Fax-Nummer verwenden.

- Klicken Sie im Windows-Startmenü auf **Programme** ➧ **RVS-COM Lite** ➧ **Neues Fax erstellen**.

  Das Fenster **RVS Fax: Empfänger** erscheint.
- Geben Sie Name des Empfängers und Rufnummer ein, z. B. ***967310***.
- Klicken Sie auf **Weiter**.
- Geben Sie einen Betreff und einen kurzen Text ein, z. B. ***Testfax***.
- Klicken Sie auf **Weiter**.
- Wählen Sie das Deckblatt **Normal**.
- Klicken Sie auf **Weiter**.
- Wenn Sie wollen, können Sie jetzt noch eine Datei anhängen, die Sie mit Ihrem Fax zusammen verschicken.
- Klicken Sie auf **Weiter** und anschließend auf **Senden**.

  Der RVS Mail Spooler erscheint und informiert Sie über den Status des gesendeten Faxes.

  Wenn Sie an sich selbst ein Fax geschickt haben, sollten Sie das Fax umgehend erhalten (vgl. Kapitel 3.8.4, Seite 78). So können Sie am besten kontrollieren, ob Ihre Fax-Anwendung funktioniert.

Sie können von jeder beliebigen Anwendung (z. B. Word) aus faxen:

- Verfassen Sie dazu (z. B. in Word) Ihre Fax-Nachricht.
- "Drucken" Sie das Dokument, indem Sie den Druckertreiber RVS Fax von RVS-COM Lite verwenden. Klicken Sie dazu im Menü **Datei** auf **Drucken** und stellen Sie den Druckertreiber **RVS Fax** ein.
- Bestätigen Sie den Druckauftrag.

  Danach erscheint das Fenster **RVS Fax: Empfänger**, das Sie gerade schon kennengelernt haben.

3.8.4 Ein Fax empfangen

Da es sich bei der Fax-Lösung mit **BinGO!** und RVS-COM Lite um eine Softfax-Lösung handelt, muß die Fax-Software immer gestartet sein, wenn Sie Faxe empfangen wollen. Bei der Installation von RVS-COM Lite wird in der Taskleiste von Windows automatisch RVS-COM Lite abgelegt – solange Sie RVS-COM Lite nicht beenden, ist die Applikation jederzeit empfangsbereit.

Alle eingehenden und ausgehenden Faxe (auch Versandfehler) werden in der RVS-COM Inbox angezeigt; ebenso Sprachnachrichten, die Sie über Ihren RVS-COM Anrufbeantworter erhalten.

➤ Klicken Sie im Windows-Startmenü auf **Programme** ➧ **RVS-COM Lite** ➧ **Inbox**.

In der Inbox sind alle bereits empfangenen Faxe und Sprachnachrichten aufgelistet:

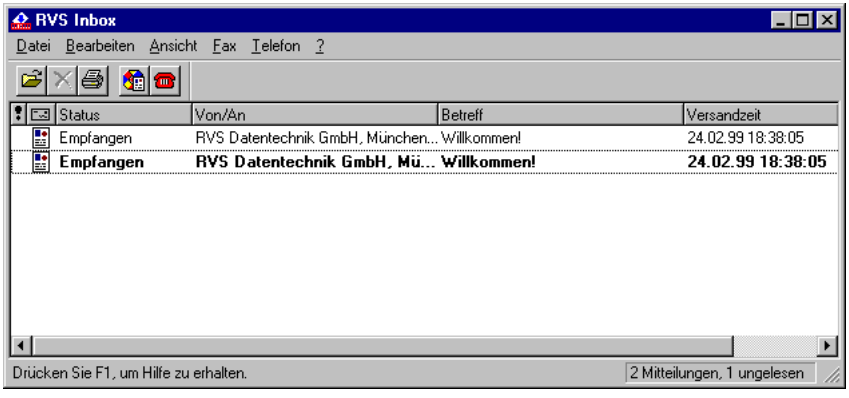
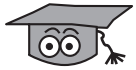


Bild 3-17: RVS Inbox

➤ Mit einem Doppelklick öffnen Sie bereits empfangene Faxnachrichten und sehen Sie im RVS Fax Viewer an (inclusive der von RVS-COM angelegten Testnachrichten).

Wenn Sie sich selbst ein Fax geschickt haben, dann sollte dort bald Ihr Fax erscheinen.

4 Grundlagen



Damit Sie einige Zusammenhänge und die Funktionsweise von **BinGO!** besser verstehen, erklären wir in diesem Kapitel einige Grundlagen über **BinGO!** und Netzwerktechnik im Allgemeinen.

Falls Sie sich während der Konfiguration in Kapitel 3, Seite 35 die nachfolgend formulierten Fragen gestellt haben, sollten Sie dieses Kapitel gründlich lesen. Es trägt sowohl zum Verständnis der weiteren Kapitel bei, hilft aber auch, Zusammenhänge des letzten Kapitels zu verstehen.

- Was ist ISDN?
- Was ist Komprimierung?
- Was sind Dienste, was Benutzer?
- Wie funktioniert Routing? Was sind Routen und Default-Routen?
- Was ist ein DHCP-Server?
- Wie funktioniert Namensauflösung?
- Wie funktionieren Filter, was ist NetBIOS?
- Was sind MIB und SNMP?

Falls Sie alles noch genauer wissen wollen, als wir es hier beschreiben, dann sollten Sie sich unsere Software Reference zu Gemüte führen. Dort finden Sie alle technischen Zusammenhänge im Detail beschrieben.

4.1 ISDN-Grundlagen

Was ist ISDN?

ISDN bedeutet Integrated Services Digital Network und beschreibt einen Telekommunikationsdienst, der weltweit unterstützt wird.

Gegenüber der bisherigen analogen Übertragung von Daten, erlaubt ISDN – wie der Name schon sagt – eine digitale Datenübertragung. Die Daten werden zwar weiterhin über die bestehenden Leitungen geschickt, aber nicht in Form von analogen Signalen, sondern eben digital. Daten, die Sie von Ihrem Rechner aus digital verschicken (z. B. E-Mail), müssen nicht erst wie bei einem Modem in Töne umgewandelt werden.

Um Daten über ISDN zu übertragen, wird am häufigsten das Protokoll ➤➤ **PPP** verwendet, Point-to-Point Protocol.

Jeder ISDN-Basisanschluß (S_0-Anschluß) besteht aus drei Kanälen:

- 2 B-Kanäle
- 1 D-Kanal

B-Kanal Kanalbündelung

Die B-Kanäle dienen der Datenübertragung (Sprache, Text, Daten). Jeder B-Kanal hat eine Datenübertragungsrate von 64 kbit/s. Da Sie zwei B-Kanäle haben, können Sie wie Sie sicherlich wissen, von zwei Telefonen aus gleichzeitig mit verschiedenen Teilnehmern telefonieren. Auch **BinGO!** kann beide B-Kanäle gleichzeitig nutzen, um Daten mit zwei verschiedenen Gegenstellen auszutauschen. Sie können sogar beide B-Kanäle "zusammenfassen", um Daten zu einer einzigen Gegenstelle über beide Kanäle zu übertragen. Sie zahlen dann zwar für beide B-Kanäle Telefongebühren, brauchen aber zur Übertragung der Daten nur die halbe Zeit. Dies können Sie bei **BinGO!** über die Funktion Kanalbündelung erreichen. Kanalbündelung können Sie nur mit dem Setup Tool konfigurieren. (Vgl. Kapitel 7.2.2, Seite 202)

D-Kanal

Der D-Kanal übermittelt Steuerinformationen mit einer Datenübertragungsrate von 16 kbit/s. Solche Steuerinformationen dienen z. B. der Identifizierung des Anrufers (Calling Party's Number = Nummer des Anrufers) und des Angerufenen (Called Party's Number = Nummer des Angerufenen) über deren Rufnummern. Z. B. können Sie Ihren Router so konfigurieren, daß er nur Gespräche von Partnern entgegennimmt, bei denen die über den D-Kanal gemeldete Rufnummer mit der Rufnummer übereinstimmt, die Sie für den Partner definiert ha-

ben. Man nennt diesen Sicherheitsmechanismus Calling Line Identification – kurz CLID. Andere Authentisierungsmechanismen überprüfen Benutzername und Paßwort der Gegenstelle. Die Überprüfung von Benutzername und Paßwort findet anhand von sogenannten ➤➤ **PAP/CHAP**-Aushandlungen statt.

CLID können Sie nur im Expert-Modus des Configuration Wizard oder im Setup Tool einstellen. PAP/CHAP-Aushandlung hingegen haben Sie bereits im Quick-Modus mit dem Wizard eingestellt.

Der Vorteil dieser Überprüfungsmechanismen ist, daß die Überprüfung bereits frühzeitig im D-Kanal stattfindet und somit eine erhöhte Sicherheit bietet.

Gebühreninformation und Shorthold

Bei vielen ISDN-Anschlüssen erhalten Sie Gebühreninformationen. Meistens erhalten Sie diese Informationen am Ende einer Verbindung, bei einigen ISDN-Anschlüssen sogar während einer Verbindung (AOCD; diese Funktion müssen Sie oft gesondert beantragen). **BinGO!** kann diese Informationen auswerten, damit Sie Kosten sparen.

Normalerweise (im Quick-Modus) ist **BinGO!** so konfiguriert, daß er nach einer bestimmten Zeit (standardmäßig 20 Sekunden) die Verbindung beendet, wenn keine Daten mehr fließen. Nach diesem festen Zeitraum, in dem keine Daten mehr ausgetauscht werden, baut **BinGO!** die Verbindung ab – auch wenn gerade ein neues Gebührenintervall angebrochen ist (statischer Shorthold).

Wenn Sie nun sicher wissen, daß Sie während einer Verbindung Gebühreninformationen bekommen, können Sie diesen Verbindungsabbau weiter optimieren und gerade angebrochene Einheiten noch ausnützen. Wenn **BinGO!** regelmäßig Gebühreninformationen durch das ISDN erhält, können Sie Ihrem Router sagen, daß er eine Verbindung erst kurz vor Beginn der nächsten Gebühreninformationen abbauen soll (dynamischer Shorthold). Die Angabe der Zeitspanne erfolgt hier nicht in Sekunden, sondern in Form eines Prozentwertes, der sich an einem Gebührenintervall orientiert (z. B. soll die Verbindung abgebaut werden, wenn 80% eines Gebührenintervalls verbraucht ist). Den dynamischen Shorthold können Sie nur im Expert-Modus des Configuration Wizard oder im Setup Tool einstellen. (Vgl. Kapitel 6.2.1, Seite 152)

Wenn Sie den dynamischen Shorthold zusätzlich zum statischen verwenden, sollte der statische immer länger als ein Gebührenintervall sein, da sonst die Wirkungsweise des dynamischen Shorthold aufgehoben ist.

Rufnummern MSN

Bei einem normalen ISDN-Basisanschluß erhalten Sie in der Regel (in Deutschland) drei Rufnummern, die sogenannten MSNs (MSN = Multiple Subscriber Number). Die MSN ist eine komplette Rufnummer ohne Vorwahl. Wenn Ihnen drei Rufnummern nicht ausreichen, können Sie normalerweise von Ihrer Telefongesellschaft weitere MSNs anfordern.

Im Quick-Modus des Configuration Wizard haben Sie Ihre Rufnummern eingetragen. Wir hatten angegeben, daß es genügt, nur jeweils die Stellen anzugeben, in denen sich die Rufnummern unterscheiden (meist die letzten beiden Stellen). **BinGO!** beginnt die Überprüfung der Rufnummern normalerweise von hinten (Modus left to right). Sobald die in der Konfiguration eingetragene Nummer der eingehenden Nummer entspricht, kann der Ruf einem Dienst eindeutig zugeordnet werden. Sie müssen daher nicht jedesmal die kompletten MSNs eintragen.

Wenn Sie Nebenstellenanlagen verwenden, kann die Sachlage etwas komplizierter sein. Bei einer Nebenstellenanlage haben Sie normalerweise eine Basisrufnummer und mehrere Durchwahlnummern. Hier sollten Sie sich auf jeden Fall über Besonderheiten Ihres Anschlusses erkundigen. Es kann nämlich sein, daß Rufnummern intern (S_0-Bus) bei verschiedenen Nebenstellenanlagen unterschiedlich gemeldet werden. Da Sie aber immer die gemeldeten Rufnummern angeben müssen, auf die **BinGO!** (oder auch RVS-COM Lite) reagieren soll, sollten Sie diese gemeldeten Rufnummern wissen. Falls Sie nicht wissen, wie Ihre Nebenstellenanlage die Rufnummern weiterreicht, können Sie das auch über **BinGO!** herausfinden (siehe Kapitel 6.1.4, Seite 133).

4.2 Wenn es noch schneller gehen soll...

Mit Kompressionsverfahren erreichen Sie in der gleichen Zeit einen höheren Datendurchsatz. Bei Kompressionsverfahren müssen Sie aber immer sicherstellen, daß Ihre Gegenstelle das entsprechende Kompressionsverfahren unterstützt. Sonst kommt keine Verbindung zustande. Im Quick-Modus des Configuration Wizard haben Sie keine Komprimierung aktiviert. Dazu müssen Sie den Expert-Modus oder das Setup Tool verwenden. (Vgl. Kapitel 7.2.7, Seite 212)

BinGO! unterstützt:

- Van Jacobsen Header-Komprimierung (VJHC):
  Komprimieren des Kopfes eines IP-Paketes.
- STAC-Datenkompression:
  Komprimieren des gesamten IP-Paketes.

4.3 Dienste und Benutzer

Abwicklung eines Anrufs

Jeder Router benutzt intern einen Algorithmus, um auf eingehende Rufe aus dem ISDN zu reagieren. **BinGO!** kann die eingehenden Rufe auf folgende Dienste verteilen:

- PPP (Routing)
- ISDN-Login
- CAPI

Was also macht so ein Dienst?

Der Dienst PPP ist der allgemeine Routing-Dienst von **BinGO!**. Damit wird eingehenden Daten-Rufen von WAN-Partnern eine Wählverbindung mit Ihrem LAN ermöglicht. So können Sie es Partnern außerhalb Ihres lokalen Netzwerkes ermöglichen, auf Rechner in Ihrem LAN zuzugreifen.

Der Dienst ISDN-Login ermöglicht eingehenden Daten-Rufen Zugang zur SNMP-Shell von **BinGO!**. So kann **BinGO!** z. B. aus der Ferne konfiguriert und gewartet werden.

Der Dienst CAPI ermöglicht eingehenden Daten- und Sprach-Rufen eine Verbindung mit Kommunikationsanwendungen auf Hosts im LAN, die auf die Remote-CAPI-Schnittstelle von **BinGO!** zugreifen. So können beispielsweise mit **BinGO!** verbundene Hosts Faxe empfangen.

CAPI und Remote-CAPI

Die meisten Anwendungsprogramme, die Kommunikationsanwendungen am Rechner ermöglichen, verwenden die genormte CAPI-Schnittstelle. Mit ihr sind die typischen Dienste, wie Anrufbeantworter, Fax G3 und G4, Dateitransfer und Euro-Filetransfer über ISDN möglich. Die CAPI-Schnittstelle alleine ermöglicht nur jeweils einem Rechner die Dienste über den ISDN-Anschluß zu nutzen. Mit Unterstützung der BinTec-eigenen Remote-CAPI ist es allen Teilnehmern im Netz möglich, diese Dienste zu nutzen, sofern jeder Teilnehmer die entsprechende Anwendersoftware installiert hat. Alle Teilnehmer teilen sich einen einzigen ISDN-Anschluß.

Was haben Sie konfiguriert?

Mit dem Configuration Wizard haben Sie im Quick-Modus die Dienste PPP (Routing) und CAPI festgelegt. ISDN-Login können Sie nur im Expert-Modus oder im Setup Tool aktivieren. Standardmäßig (die Zuordnung können Sie nur

im Expert-Modus ändern) teilt der Configuration Wizard die Nummern den Diensten folgendermaßen zu:

Rufnummer	Datendienste	Sprachdienste
1 (z. B. ***10***)	PPP (Routing)	CAPI
2 (z. B. ***11***)	CAPI	CAPI
3 (z. B. ***12***)	CAPI	CAPI

Ein WAN-Partner könnte Sie jetzt theoretisch unter der Nummer ***10*** anrufen, um auf Daten Ihres Netzes zuzugreifen – sofern Sie ihn als WAN-Partner definiert haben.

Unter den Nummern ***11*** und ***12*** können Sie Daten- und Sprachdienste in RVS-COM Lite einrichten.

In unserem Konfigurationsbeispiel (vgl. Bild 3-12, Seite 72) haben wir die Nummer ***10*** als Faxnummer verwendet und die Nummer ***11*** für einen Anrufbeantworter. Wie Sie sicherlich bemerkt haben, ist die Nummer ***10*** zwei mal vergeben: für PPP und CAPI.

Sprache oder Daten?

Da bei der Rufannahme außer der Rufnummer auch zwischen Daten- und Sprachrufen unterschieden wird, ist diese Doppelbelegung für **BinGO!** kein Problem. **BinGO!** erkennt bei einem eingehenden Fax auf der Nummer ***10***, daß es sich um Sprachdaten (Töne) handelt und leitet die Informationen an den CAPI-Dienst weiter. Wenn sich hingegen ein WAN-Partner in Ihr Netz einwählt, handelt es sich um digitale Informationen (Daten) und **BinGO!** leitet die Daten an den Dienst PPP.

Daten sind:

- Digitaler Datenaustausch (PPP Routing)
- Fax G4 (digitales Fax)

Sprache sind:

- Sprache (Telefonieren)
- Fax G3 (herkömmliches Fax)
- Modem

Wer ist schneller?

Wir sind außerdem davon ausgegangen, daß Sie unter der Nummer ***11*** auch über ein Telefon erreichbar sind, das am gleichen S_0-Bus angeschlossen ist wie **BinGO!**. Alle Geräte, die am gleichen S_0-Bus angeschlossen sind und die unter der gleichen Rufnummer erreichbar sind, reagieren auch auf Anrufe. D. h. bei einem eingehenden Ruf unter der Nummer ***11*** klingelt Ihr Telefon, gleichzeitig fühlt sich aber auch RVS-COM Lite angesprochen. Da Sie bei RVS-COM Lite die Anzahl der Klingelzeichen vor der Rufannahme angegeben haben, wartet RVS-COM Lite erst einmal ab. Falls Sie den Hörer zuerst abnehmen, sind Sie schneller und erhalten den Ruf. Falls Sie nicht rechtzeitig am Apparat sind, bevor die Anzahl der Klingelzeichen von RVS-COM Lite erreicht ist, ist RVS-COM Lite schneller und nimmt den Ruf entgegen.

Mehrere Benutzer

Eine Rufnummer haben wir nicht besetzt: die ***12***. Falls Sie ein Netzwerk mit zwei Rechnern im LAN haben, könnten Sie theoretisch jedem dieser zwei Rechner eine eigene Faxnummer zuweisen. Im CommCenter von Rechner 1 würden Sie weiterhin die ***11*** als Rufnummer eingetragen lassen, im CommCenter von Rechner 2 würden Sie die Nummer ***12*** als Rufnummer für Fax eintragen (vgl. Bild 4-1, Seite 86).

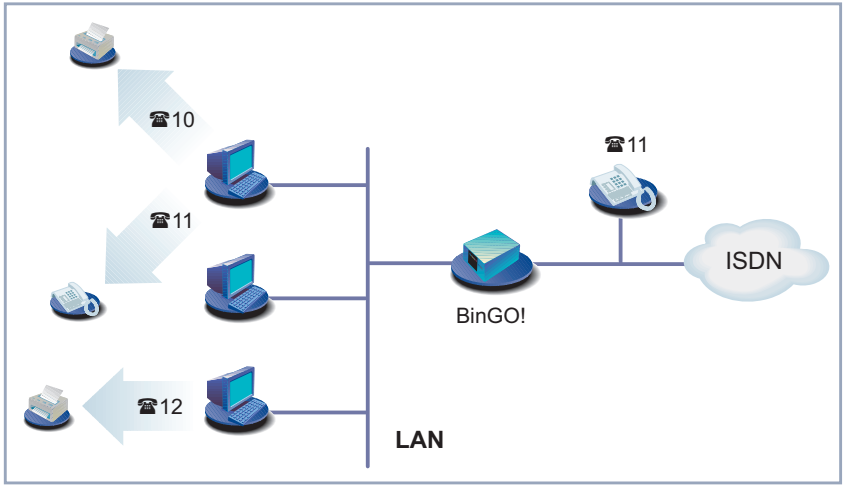


Bild 4-1: Szenario: 2 Rechner, 2 Fax-Nummern, 1 Telefon

Dies funktioniert bereits sehr gut. Aber angenommen, einer der beiden Teilnehmer an Rechner 1 oder Rechner 2 ändert die Rufnummer! Beide CommCenter

würden z. B. auf einen eingehenden Ruf unter der Nummer ***11*** reagieren. Wer schneller ist, bekommt das Fax...

Dies ist zwar ärgerlich, aber nicht unbedingt sicherheitskritisch. Vielleicht haben Sie aber auch Daten, die auf keinen Fall Dritte einsehen sollen?

Mehr Sicherheit

Wenn Sie von vornherein festlegen wollen, daß bestimmte Daten-/Sprachrufe bei einem der beiden CommCenter von RVS-COM Lite gar nicht erst ankommen, können Sie den Zugang durch einen Benutzernamen und ein Paßwort schützen. Das CAPI User Concept hilft Ihnen aus der Patsche:

Default Nutzerkonto

Im Quick-Modus haben Sie das sogenannte Default Nutzerkonto angelegt. Dies ist eine einfache Konfigurationsmöglichkeit. Alle Anwender im Netz können die Kommunikationsanwendungen über die Remote-CAPI-Schnittstelle verwenden. Es wird ein Default-Nutzer ohne Paßwort im CAPI-Konfigurationsprogramm und auf dem Router eingetragen. Alle im Netz sind gleichberechtigt.

Mehrere Nutzerkonten

Jeder Anwender, dem bestimmte Kommunikationsanwendungen gestattet werden sollen, erhält einen eigenen Benutzernamen und ein eigenes Paßwort. Die Einstellungen für Name und Paßwort müssen Sie auf dem Router (z. B. über den Configuration Wizard im Expert-Modus oder im Setup Tool Kapitel 7.1.2, Seite 192) und auf dem jeweiligen Rechner vornehmen (Remote-CAPI-Konfiguration). Zusätzlich bestimmen Sie auf dem Router für jeden Anwender eine eigene Rufnummer (z. B. Fax-Nummer). Auf die Rufnummer reagiert nur die Kommunikationsanwendung des Rechners, bei dem auch in der CAPI-Konfiguration der zugehörige Nutzer eingetragen ist.

4.4 BinGO! als DHCP-Server

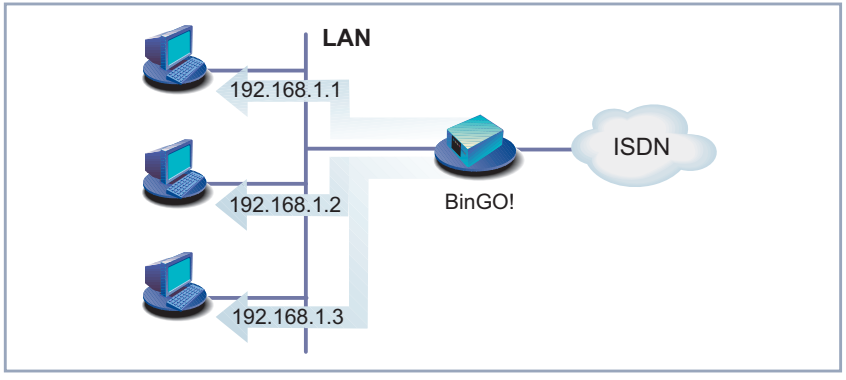


Bild 4-2: **BinGO!** als DHCP-Server

Wozu IP-Adressen?

Jeder Rechner in Ihrem LAN benötigt, wie auch **BinGO!**, eine eigene Adresse. Sonst können die Geräte untereinander nicht kommunizieren. Wenn Sie einen Brief mit der Post verschicken, müssen Sie auch Absender und Adressat angeben – andernfalls kommt der Brief weder an, noch kann er an Sie zurückgeschickt werden.

In einem TCP/IP-Netzwerk werden für solche Zwecke IP-Adressen verwendet. In anderen Netzen, z. B. IPX- oder X.25-Netze, funktioniert das ähnlich. Mehr zu IP-Adressen erfahren Sie unserer Software Reference.

Woher weiß ich, wer ich bin?

Diese IP-Adressen können Sie auf Ihrem Rechner fest einrichten. Der Nachteil: Wenn Sie Ihr Netzwerk neu einrichten oder umkonfigurieren, müssen Sie jedem Rechner einzeln sagen, welche IP-Adresse er hat. Wenn Sie mehrere Rechner im Netzwerk haben, kann das viel Arbeit bedeuten.

Mit einem DHCP-Server (DHCP = Dynamic Host Configuration Protocol) verringert sich Ihr Aufwand. Der DHCP-Server nimmt Ihnen fast die ganze Arbeit ab. Ein DHCP-Server vergibt allen Rechnern im LAN automatisch IP-Adressen. Die Rechner sind dann DHCP-Clients. Alles, was Sie tun müssen, ist einmalig einen Pool an IP-Adressen zu definieren, die der DHCP-Server an Geräte im Netzwerk vergeben darf. Zusätzlich müssen Sie den Rechnern mitteilen, daß Sie Ihre IP-Adresse vom Server anfordern sollen.

BinGO! kann nicht als DHCP-Ciient eingerichtet werden. Es ist aber möglich, **BinGO!** über einen BootP-Server eine IP-Adresse zuzuweisen. (Vgl. Kapitel 5.1.2, Seite 105)

Innerhalb eines Netzes dürfen nicht mehrere DHCP-Server mit den gleichen Adreß-Pools sein.

BinGO! als DHCP-Server

Sie können **BinGO!** als DHCP-Server verwenden, wenn Sie keinen anderen DHCP-Server haben (vgl. Kapitel 6.1.5, Seite 143). Er vergibt an alle Geräte des eigenen Netzes IP-Adressen. Eventuell haben Sie im Quick-Modus mit dem Configuration Wizard **BinGO!** bereits als DHCP-Server eingerichtet. Wenn Sie die vorgeschlagenen Werte übernommen haben, dann erhalten jetzt Ihre Rechner IP-Adressen von ***192.168.1.1*** bis ***192.168.1.8***.

Wann werden IP-Adressen zugeteilt?

Jeder Rechner, der sich neu am Netz anmeldet – weil er z. B. neu gestartet wurde – sendet einen Adreß-Request aus und erhält daraufhin seine IP-Adresse. Diese Adresse erhält der Rechner meist nur für einen definierten Zeitraum (im Setup Tool können Sie diesen Zeitraum einstellen). Danach wird die Adresse neu zugewiesen. Sie können Ihrem Rechner aber auch explizit sagen, daß er jetzt eine IP-Adresse bekommen soll. Dies hat der Configuration Wizard im Quick-Modus für Sie getan, falls Sie **BinGO!** als DHCP-Server eingerichtet haben.

Unter Windows 95 rufen Sie das Programmen WINIPCFG auf, um IP-Adressen zu überprüfen oder neu zuzuweisen. Unter Windows NT verwenden Sie das Programm IPCONFIG.

WINIPCFG aufrufen

- Klicken Sie im Windows-Startmenü auf **Ausführen**.
- Geben Sie `winipcfg` ein.

  Es erscheint ein Fenster, in dem Sie die IP-Adresse Ihres Rechner und andere Netzinformationen sehen.
- Um eine IP-Adresse neu zuzuweisen, klicken Sie auf **Renew**.

IPCONFIG aufrufen

- Klicken Sie im Windows-Startmenü auf **Programme** ➧ **Eingabeaufforderung**.

- Geben Sie `ipconfig` oder `ipconfig/all` ein, um die IP-Adresse Ihres Rechners und andere Netzinformationen abzufragen.
- Geben Sie `ipconfig/renew` ein, um eine IP-Adresse neu zuzuweisen.
- Geben Sie `ipconfig/release` ein, um eine IP-Adresse freizugeben.

4.5 Wie funktioniert Namensauflösung?

Nun haben Sie viel darüber gehört, wozu Sie eine IP-Adresse benötigen. Was aber, wenn Sie nun mit dem Rechner ***BossPC*** plaudern wollen oder die Internetseiten von ***www.bintec.de*** ansehen wollen? ***BossPC*** und ***www.bintec.de*** sind offensichtlich keine IP-Adressen, sondern Namen. Da aber Rechner nur IP-Adressen und keine Namen verstehen, muß es eine Stelle geben, welche die zu den Namen gehörigen IP-Adressen bekannt gibt – eine Namensauflösung durchführt.

Namensauflösung

Für Namensauflösung gibt es verschiedene Möglichkeiten, z. B.:

- DNS-Server (im LAN, beim Internet Service Provider oder im Partnernetz)
- **BinGO!** als DNS-Proxy:
  - Auf dem PC ist die IP-Adresse von **BinGO!** als DNS-Server eingetragen.
  - **BinGO!** ist als DHCP-Server, Ihre Rechner sind als DHCP-Clients konfiguriert und bekommen automatisch die IP-Adresse von **BinGO!** mitgeteilt, die dann für DNS-Anfragen verwendet wird.
- WINS-Server
- HOSTS- und LMHOSTS-Datei

DNS

Über den Dienst ➤➤ **DNS** werden Host-Namen bzw. Computer-Namen in IP-Adressen übersetzt. Auf einem DNS-Server legen Sie eine Art Tabelle an, in der zu Computer-/Host-Namen die zugehörigen IP-Adressen aufgeführt und bei Bedarf bekanntgegeben werden.

DNS-Server bilden einen hierarchische Baumstruktur. Sobald der primäre DNS-Server eine Anfrage erhält, versucht er den Namen aufzulösen. Kann er dies nicht, fragt er bei einem übergeordneten DNS-Server nach.

BinGO! als DNS-Proxy

Wenn Sie **BinGO!** als DNS-Proxy verwenden (Standardfall), leitet Ihr Router alle DNS-Anfragen an ihm bekannte DNS-Server weiter (im Normalfall ein DNS-Server beim Internet Service Provider).

WINS

Speziell in Windows-Netzwerken gibt den Dienst WINS. Über WINS können Sie nur Computer-Namen oder sogenannte NetBIOS-Namen auflösen, aber keine

Host-Namen. Analog zu TCP/IP wird NetBIOS als Transportprotokoll verwendet. Meist sind in Windows-Netzwerken Computer- und Host-Namen identisch.

HOSTS- und LMHOSTS-Datei

Die LMHOSTS-Datei haben Sie eventuell im vorherigen Kapitel schon kennengelernt. In einer LMHOSTS-Datei legen Sie eine Tabelle von Computer-Namen und zugehörigen IP-Adressen an. Die HOSTS-Datei ist ähnlich aufgebaut. Statt Computer-Namen übersetzt die HOST-Datei allerdings Host-Namen in IP-Adressen.

Wie funktioniert Namensauflösung in der Praxis?

Internetzugang

Wenn Sie mit dem Configuration Wizard einen Internetzugang einrichten und keinen eigenen DNS-Server haben, bezieht **BinGO!** normalerweise die IP-Adresse eines Domain Name Server vom Internet Service Provider automatisch. Auf den PCs im LAN ist **BinGO!** als DNS-Proxy bekannt. Bei einer Anfrage zur Namensauflösung (z. B. für ***www.bintec.de***) fragt der PC beim Router, der Router wiederum beim DNS-Server des Internet Service Providers nach. So kann die Adresse aufgelöst werden.

Soweit ist alles klar. Was aber, wenn Sie zusätzlich eine Firmennetzanbindung konfigurieren?

Internetzugang und Firmennetzanbindung

Wenn Sie zusätzlich zur Internetanbindung eine Firmennetzanbindung einrichten, Sie **BinGO!** als DNS-Proxy verwenden und die DNS-Einstellungen von **BinGO!** zum Internet Service Provider führen (Standardfall), würden alle Anfragen zur Namensauflösung an Ihren Provider gestellt. Wenn Sie nun einen Rechner im Partnernetz (***BossPC***) erreichen wollen, würde **BinGO!** eine Verbindung zum Provider aufbauen und dort nach der IP-Adresse von ***BossPC*** fragen. Computer-Namen allerdings sind im Gegensatz zu Adressen wie ***www.binte.de*** nicht im Internet bekannt. Sie werden nur innerhalb eines Firmennetzes verwendet (Domäne, Arbeitsgruppe). Der Domain Name Server beim Provider könnte deshalb den Namen normalerweise nicht auflösen. Der Verbindungsaufbau wäre unnötig, Sie können ***BossPC*** trotzdem nicht erreichen.

Damit solche ungewollten und nutzlosen Verbindungen nicht zustande kommen, müssen Sie verhindern, daß solche Anfragen zu Rechnern Ihres Partnernetzes nicht gestellt werden. Diese Aufgabe übernimmt der einfache NetBIOS-Filter für Sie (siehe Kapitel 4.7, Seite 97), den Sie mit dem Configuration Wizard konfiguriert haben.

Dies allerdings löst nicht Ihr Problem. Sie wollen ja immer noch zu dem Namen ***BossPC*** die IP-Adresse wissen.

Eine Lösungsmöglichkeit wäre: Sie richten sich einen eigenen Domain Name Server ein, in dem alle Zuordnungen (Rechner des Partnernetzes und deren IP-Adressen) zu finden sind, die Sie erreichen wollen. Da es allerdings in einem kleinen Netzwerk nicht immer sinnvoll ist, für ein oder zwei solcher Zuordnungen einen eigenen Server einzurichten, gibt es auch eine zweite Möglichkeit:

Sie speichern die Zuordnung IP-Adresse zu Name auf Ihrem Rechner ab. Dies müssen Sie dann allerdings auf allen Rechnern tun, die diese Informationen benötigen. Die LMHOSTS-Datei können Sie für solche Zwecke verwenden.

Wie Sie in der LMHOSTS-Datei einen Eintrag erstellen, haben wir bereits in Kapitel 3.6.2, Seite 64 erklärt.

Damit unsere Lösung funktioniert, sollten Sie allerdings noch einige Punkte beachten:

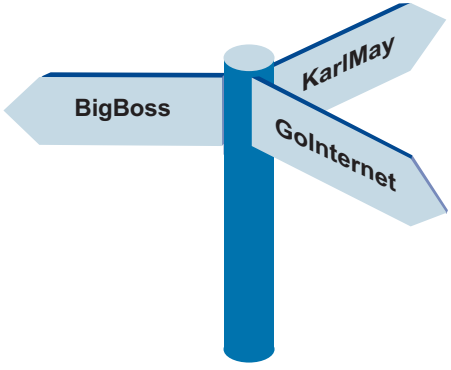
- Domänen- und Arbeitsgruppen-Namen müssen in Ihrem und im Partnernetz gleich sein.
- Sie müssen beim Partnernetz als Benutzer bekannt sein.
- Sie dürfen mit dem Configuration Wizard keine umfangreiche NetBIOS-Filterung eingestellt haben, sonst können bestimmte Windows-Funktionen wie z. B. eine Netzlaufwerksverbindung nicht genutzt werden.

Das Thema "Verbindung von Windows-Netzwerken" ist sehr komplex und umfangreich. Eine Reihe von Faktoren bestimmen den Erfolg eines solchen Vorhabens. Da eine genauere Behandlung dieses Themas den Rahmen unseres Handbuches sprengen würde, können wir an dieser Stelle nur auf andere Fachliteratur verweisen, z. B. "Windows NT 4.0 Connectivity Guide" von Richard Grace (ISBN 0-7645.3160-3).

4.6 Was sind Routen und Default-Routen?

Routen

Um IP-Pakete zu einem Partnernetz oder einem Internet Service Provider verschicken zu können, muß **BinGO!** wissen, welche Pakete wohin geleitet werden sollen.



Dafür definieren Sie Wege bzw. Routen. Die Routen führen zu einem bestimmten Netzwerk mit einer definierten ➤➤ **Netzadresse** und einer ➤➤ **Netzmaske**. Für jedes Netz, in das Sie gelangen wollen, geben Sie eine solche Route an. Sie bestimmen beispielsweise die Route zu Ihrem WAN-Partner (Firmenzentrale). Alle Pakete, deren IP-Adressen zur Netzmaske und Netzadresse dieser Route passen, werden dann an dieses Partnernetz geschickt.

Wohin aber mit allen übrigen IP-Paketen?

Default-Route

Anhand einer sogenannten Default-Route können Sie bestimmen, daß alle Pakete, deren Ziel **BinGO!** unbekannt ist, zu einem bestimmten Netz geschickt werden (Default-Route). Üblicherweise verwendet man für die Default-Route die Route zum Internet Service Provider, da die meisten unbekannten Pakete als Ziel das Internet haben (z. B. ***www.bintec.de***). Der Configuration Wizard hat die Route zu Ihrem Provider automatisch als Default-Route eingetragen, sofern Sie einen Internetzugang eingerichtet haben. Wenn Sie nur ein Partnernetz, nicht aber einen Internetzugang einrichten, verwendet der Configuration Wizard einfach als Default-Route die Route zu Ihrem Partnernetz.

Wenn Sie keinen Internetzugang haben, hingegen Ihre Firmenzentrale einen Internet Service Provider hat, können Sie über die Firmenzentrale ins Internet.

Indem Sie die Default-Route zu Ihrer Zentrale eingerichtet haben, dort alle unbekannten Pakete ankommen, und Ihr Partnernetz wiederum alle unbekannten IP-Pakete zu einem Internet Service Provider routet, können Sie in Absprache mit Ihrem WAN-Partner über das Partnernetz ins Internet.

Mehrere Routen für einen WAN-Partner

Das Netzwerk der Firmenzentrale kann aus mehreren LANs mit unterschiedlichen Netzadressen und Netzmasken bestehen (Subnetze). In diesem Fall müssen Sie für jedes Subnetz, das Sie in der Firmenzentrale erreichen wollen, eine eigene Route angeben (vgl. Bild 4-3, Seite 95).

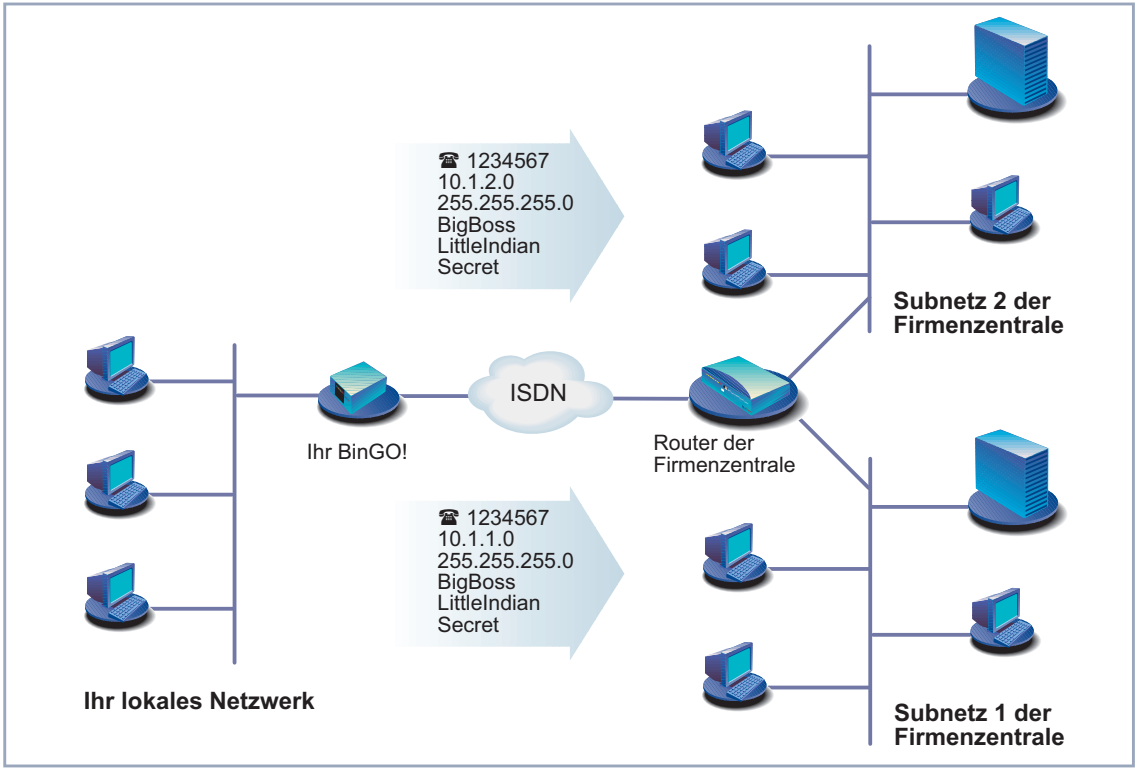


Bild 4-3: Szenario: WAN-Partner mit zwei Subnetzen

Routen, Namensauflösung und Gateway

Nicht nur **BinGO!**, sondern auch Ihre Rechner kennen so etwas wie eine Default-Route: das Gateway. Alle Pakete, deren Ziel nicht innerhalb des eigenen Netzes liegt, schickt Ihr Rechner zu diesem Gateway. Als Gateway dient **BinGO!**. Sobald Ihr Router ein solches Paket empfängt, schickt er es wiederum über eine seiner Routen (z. B. zum Internet Service Provider oder einem anderen Partnernetz) weiter.

Angenommen **BinGO!**'s Default-Route führt zum Internet Service Provider, Ihre Rechner sind DHCP-Clients und bekommen ihre IP-Adresse von **BinGO!**

zugewiesen. In diesem Fall bekommen die Rechner auch die IP-Adresse von **BinGO!** als DNS-Proxy und Gateway mitgeteilt. (Das Beispiel funktioniert auch, wenn Ihre PCs keine DHCP-Clients sind, aber so konfiguriert sind, daß die IP-Adresse von **BinGO!** als DNS-Server und Gateway eingetragen ist.)

Sobald Sie z. B. ***www.bintec.de*** im Browser eingeben, schickt der PC eine DNS-Anfrage an **BinGO!** – **BinGO!** ist ja als DNS-Proxy bekannt. **BinGO!** selbst schickt als DNS-Proxy das Paket mit der DNS-Anfrage zum Internet Service Provider. Dort kann der Name ***www.bintec.de*** aufgelöst werden, die DNS-Anfrage ist erfolgreich und der Rechner erhält als Antwort die IP-Adresse zum Namen ***www.bintec.de*** zurück. Nun kann das Paket auf die eigentliche Reise zu ***www.bintec.de*** geschickt werden. Da **BinGO!** als Gateway eingetragen ist, und das Paket eine IP-Adresse hat, die nicht innerhalb des eigenen Netzes liegt, wird das Paket über das Gateway **BinGO!** nach außen geschickt. Da für die IP-Adresse zu ***www.bintec.de*** keine eigene Route eingetragen ist, verwendet **BinGO!** die Default-Route.

4.7 Filter und NetBIOS

Gerade haben Sie viel über Namensauflösung und Routen erfahren. Das ist alles sehr praktisch, aber...

Warum Filter? Jedes Windows-Netzwerk verwendet Computer-Namen. Z. B. heißt Ihr Rechner Winnetou, ein anderer Rechner im Netz OldShatterhand. Diese Computer-Namen sind nicht im Internet bekannt, das Sie nur innerhalb eines Firmennetzes verwendet werden (anders als bei Adressen wie ***www.bintec.de***). Diese Computer-Namen werden in jedem Windows-Netzwerk über den Dienst NetBIOS aufgelöst. NetBIOS wiederum versucht, diese Computer-Namen über Ihren Internet Service Provider aufzulösen. **BinGO!** würde ständig (die Abfragen sind ca. alle 12 bis 15 min und somit recht häufig!) eine unnötige Verbindung mit Ihrem Provider herstellen, da der Provider die WINS-Namen nicht auflösen kann. Die Namen sind ja nur in Ihrem Netz (Arbeitsgruppe, Domäne) bekannt.

Hier kommen die Filter ins Spiel.

Einfacher Filter Wenn Sie mit dem Configuration Wizard den einfachen NetBIOS-Filter aktiviert haben, werden alle IP-Pakete verworfen, die zu **BinGO!** für eine NetBIOS-Namensauflösung geschickt werden. Der Configuration Wizard konfiguriert im Quick-Modus immer eine einfache Filterung.

Umfangreicher Filter Die umfangreiche Filterung können Sie nur im Expert-Modus oder mit dem Setup Tool vornehmen. Beim umfangreichen Filter wird der ganze NetBIOS-Datenverkehr (NetBIOS-Broadcasts) gefiltert – also nicht nur die Anfragen zur Namensauflösung. Einziger Nachteil: Sobald mehrere WAN-Partner (z. B. Internet- und Firmennetzanbindung) eingerichtet sind, können alle Dienste von NetBIOS wie das gemeinsame Nutzen von Laufwerken und Druckern nicht verwendet werden.

CAPI-Filter Zusätzlich können Sie im Expert-Modus mit dem Configuration Wizard auch noch einen CAPI-Filter einrichten. Nehmen wir an, Sie haben in Ihrer CAPI-Konfiguration statt der IP-Adresse von **BinGO!** aus Versehen eine falsche IP-Adresse eingegeben. Ihre Rechner würden CAPI-Anfragen immer an die falsche Adresse schicken. Da die falsche IP-Adresse sich vielleicht außerhalb Ihres Netzes befindet, versucht **BinGO!**, das entsprechende IP-Paket an Ihren Internet Service Provider zu leiten. Also wieder ein unnötiger Verbindungsauf-

bau. Der CAPI-Filter bewirkt, daß CAPI-Anfragen, die nicht innerhalb des eigenen Netzes bleiben, verworfen werden.

Mit Filter-Mechanismen können Sie nicht nur ungewollte Verbindungen vermeiden. Die primäre Funktion von Filtern ist Sicherheit des eigenen Netzes vor Zugriffen von außen. (Vgl. Kapitel 8.2.8, Seite 250)

4.8 MIB und SNMP

Was ist SNMP?

SNMP (Simple Network Management Protocol) ist ein Protokoll, das zur Protokollfamilie TCP/IP gehört. Mit Hilfe von SNMP werden Managementinformationen von Netzwerkkomponenten (z. B. Router, Drucker, Rechner) in einem Netz transportiert. Es wird verwendet, um die Geräte in einem Netzwerk zu überwachen und zu verwalten. Die Überwachung erfolgt dabei von zentraler Stelle aus über einen SNMP-Manager. Dieser SNMP-Manager ist ein Programm, das über SNMP Daten von den Geräten im Netz anfordern kann. Ein Administrator, der diesen SNMP-Manager bedient, kann alle Geräte in seinem Netz von einem Standort aus überwachen. SNMP definiert als Protokoll die Regeln, mit denen sich dann das Managementprogramm mit den Clients (z. B. **BinGO!**) unterhält. Auf Ihrer BinTec Companion CD befindet sich ein solcher SNMP-Manager, der DIME Browser (für Windows-Betriebssysteme). Statt dem DIME Browser können Sie zur Verwaltung Ihres Netzes aber auch jeden anderen beliebigen SNMP Manager verwenden, z. B. HP OpenView. Statt eines graphisch orientierten Programmes können Sie sogar auch direkt auf Kommandozeilen-Ebene arbeiten (SNMP Shell).

Was ist MIB?

Wir haben gerade erklärt, daß über SNMP in einem Netzwerk Managementinformationen ausgetauscht werden. Was nun aber sind Managementinformationen? Nun, der Name MIB ist eine Kurzform für Management Information Base und hat daher unmittelbar etwas mit diesen Managementinformationen zu tun.

In einer MIB sind Objekte gespeichert (Information Base), die über SNMP abgefragt, geändert oder erzeugt werden können (Management). Die Objekte selbst sind Informationscontainer, in die Informationen abgelegt werden, um Zustände und Werte des Objekts zu definieren. Ein Objekt, das Sie selbst bei der Konfiguration Ihres Routers mit dem Configuration Wizard geändert haben, ist z. B. das Objekt, in dem Ihre Zugangsberechtigung zu **BinGO!** abgelegt ist. Ursprünglich war der Wert bintec als Paßwort definiert, jetzt ist dort Ihr eigener Wert abgelegt.

Jedes dieser Objekte ist einzigartig und hat einen Namen, im Beispiel der Zugangsberechtigung: **bintecsec**. Ein Objekt wird auch als Tabelle bezeichnet. Jede Tabelle wiederum hat eine Anzahl von Variablen, die bestimmte Eigenschaften definieren, z. B. die Variable **biboAdmAdminCommunity**, in der nun der Wert Ihres Paßworts abgelegt ist.

5 Ein Draht zu BinGO!

In diesem Kapitel werden die verschiedenen Zugangs- und Konfigurationsmöglichkeiten erläutert.

Sie erfahren,

- wie Sie auf **BinGO!** zugreifen.
- wie Sie sich einloggen.
- welche Konfigurationsmöglichkeiten Ihnen zur Verfügung stehen.
- wie das ➤➤ **Setup Tool** aufgebaut ist.

5.1 Zugangsmöglichkeiten

Um Ihren ➤➤ **Router** konfigurieren zu können, müssen Sie auf ihn zugreifen. Dafür gibt es drei verschiedene Möglichkeiten:

- Über die serielle Schnittstelle
- Über Ihr ➤➤ **LAN**
- Über eine ➤➤ **ISDN**-Verbindung

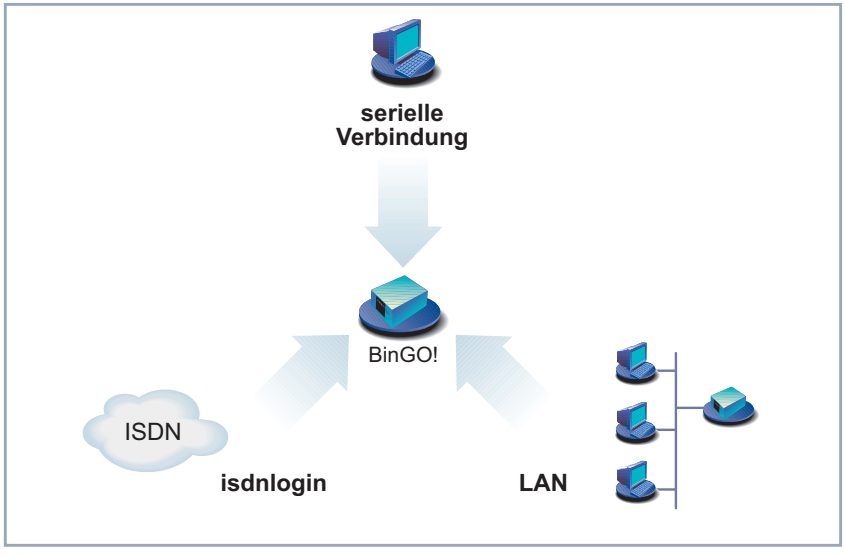


Bild 5-1: Zugangsmöglichkeiten zu **BinGO!**

Im Folgenden werden die verschiedenen Zugangsmöglichkeiten vorgestellt. Daraus können Sie das für Ihre Bedürfnisse geeignete Vorgehen auswählen. Für welchen Zugang Sie sich auch entscheiden, in jedem Fall erscheint auf Ihrem Monitor die ➤➤ **SNMP-Shell** von **BinGO!**, die Sie für die Konfiguration über das Setup Tool benötigen.

5.1.1 Zugang über die serielle Schnittstelle

Erstkonfiguration

Der Zugang über die serielle Schnittstelle ist gut geeignet, wenn Sie eine Initialkonfiguration von **BinGO!** durchführen. Um **BinGO!** über die serielle Schnittstelle an Ihren Rechner anzuschließen, gehen Sie vor wie in Kapitel 3.1, Seite 37 erläutert.

Windows

Wenn Sie einen Windows-PC benutzen, benötigen Sie für die serielle Verbindung ein Terminalprogramm, z. B. **HyperTerminal**. Dieses Hilfsprogramm haben Sie in Kapitel 3.3, Seite 46 zusammen mit der **BRICKware for Windows** installiert.

- Klicken Sie im Windows-Startmenü auf **Programme** ➧ **BRICKware** ➧ **BRICK at COM1** (bzw. **BRICK at COM2**, wenn Sie die COM2-Schnittstelle des Rechners benutzen), um **HyperTerminal** zu starten.
- Drücken Sie die **Eingabetaste** (evtl. mehrmals), wenn sich das HyperTerminal-Fenster geöffnet hat.

  Es erscheint ein Fenster mit dem Login-Prompt. Sie befinden sich auf der SNMP-Shell von **BinGO!.**
- Fahren Sie fort mit Kapitel 5.2, Seite 107.

Falls der Login-Prompt auch nach mehrmaligem Betätigen der **Eingabetaste** nicht erscheint, konnte die Verbindung zu **BinGO!** nicht hergestellt werden. Überprüfen Sie daher die Einstellungen von COM1 bzw. COM2:

- Klicken Sie auf **File** ➧ **Properties**.
- Klicken Sie im Register **Phone Number** auf **Configure**....
  Folgende Einstellungen sind erforderlich:
  - Bits per second: 9600
  - Data bits: 8
  - Parity: None
  - Stop bits: 1
  - Flow Control: None
- Tragen Sie die Werte ein und klicken Sie auf **OK**.
- Stellen Sie im Register **Settings** ein:
  - Emulation: Auto detect
- Klicken Sie auf **OK**.

Sie können auch jedes andere Terminalprogramm verwenden, das sich auf 9600 bit/s, 8N1 (8 Datenbits, No Parity, 1 Stoppbit), Softwarehandshake (XON, XOFF) und VT100-Emulation einstellen läßt.

Unix Wenn Sie einen Unix-Rechner benutzen, können Sie HyperTerminal nicht verwenden. Sie benötigen ein Terminalprogramm wie z. B. **cu** (unter System V), **tip** (unter BSD) oder **minicom** (unter Linux). Die Einstellungen für diese Programme sind die gleichen wie oben aufgelistet.

5.1.2 Zugang über LAN

Über den Dienst ➤➤ **telnet** können Sie **BinGO!** vom LAN aus erreichen. Telnet steht normalerweise auf jedem Rechner zur Verfügung. Um Ihren Router über das LAN erreichen zu können, sollte er bereits eine ➤➤ **IP-Adresse** und ➤➤ **Netzmaske** haben. Wenn dies nicht der Fall ist, **BinGO!** also noch unkonfiguriert ist, haben Sie zwei Möglichkeiten:

- Wenn Sie mit Windows arbeiten, können Sie **BinGO!** eine IP-Adresse zuweisen, bevor Sie telnet ausführen. Dazu benötigen Sie das Hilfsprogramm ➤➤ **DIME Tools**. Wenn Sie DIME Tools zusammen mit der **BRICKware for Windows** noch nicht installiert haben, gehen Sie vor wie in Kapitel 3.3, Seite 46 beschrieben.
- Wenn Sie nicht mit Windows arbeiten, verwenden Sie für die Initialkonfiguration einen anderen Zugang (über die serielle Schnittstelle oder über ISDN).

➤ Schließen Sie **BinGO!** an das LAN an wie in Kapitel 3.1, Seite 37 beschrieben.

IP-Adresse zuweisen

Gehen Sie folgendermaßen vor, um **BinGO!** mit dem Programm **DIME Tools** eine IP-Adresse zuzuweisen (falls dies nötig ist):

➤ Klicken Sie im Windows-Startmenü auf ***Programme*** ➧ ***BRICKware*** ➧ **DIME Tools**.

Nach kurzer Zeit erscheint das ➤➤ **BootP**-Server-Fenster, wenn **BinGO!** noch unkonfiguriert ist.

➤ Geben Sie in dem Fenster unter **BRICK Parameter** Name und IP Addresse von **BinGO!** ein (wenn Sie unsicher sind, beachten Sie Kapitel 3.2, Seite 40).

➤ Klicken Sie auf **OK**.

➤ Schließen Sie **DIME Tools**.

telnet ausführen

Bauen Sie nun mit telnet eine Verbindung zu **BinGO!** auf:

Windows

➤ Klicken Sie im Windows-Startmenü auf **Ausführen**....

➤ Geben Sie `telnet <IP-Adresse von BinGO!>` ein.

➤ Klicken Sie auf **OK**.

Es erscheint ein Fenster mit dem Login-Prompt. Sie befinden sich auf der SNMP-Shell von **BinGO!**. Fahren Sie fort mit Kapitel 5.2, Seite 107.

Unix

➤ Geben Sie `telnet <IP-Adresse von BinGO!>` in ein Terminal ein.

Es erscheint ein Fenster mit dem Login-Prompt. Sie befinden sich auf der SNMP-Shell von **BinGO!**. Fahren Sie fort mit Kapitel 5.2, Seite 107.

5.1.3 Zugang über ISDN

Remote-Konfiguration

Der Zugang über ➤➤ **ISDN** mit ➤➤ **ISDN-Login** empfiehlt sich vor allem dann, wenn **BinGO!** sich an einem anderen Standort befindet, und Sie ihn aus der Ferne konfigurieren oder warten wollen. Dies ist auch dann möglich, wenn **BinGO!** sich noch im Auslieferungszustand befindet. Sie müssen dazu über einen anderen, bereits konfigurierten BinTec-Router (in LAN 1) verfügen und die Rufnummer Ihres (neuen) Routers (in LAN 2) kennen. So kann z. B. der Administrator in der Firmenzentrale den Router eines Mitarbeiters im Home-Office konfigurieren, ohne vor Ort zu sein. **BinGO!** im Home-Office muß lediglich mit dem ISDN-Anschluß verbunden und eingeschaltet sein.

Der Zugang über ISDN verursacht Kosten. Wenn **BinGO!**, Router und Rechner im gleichen LAN sind, ist es billiger, auf **BinGO!** über das LAN oder über die serielle Schnittstelle zuzugreifen.

➤ Schließen Sie **BinGO!** an das ISDN an wie in Kapitel 3.1, Seite 37 beschrieben.

Gehen Sie folgendermaßen vor, um **BinGO!** über ISDN-Login zu erreichen:

➤ Loggen Sie sich wie gewohnt auf Ihrem BinTec-Router (in LAN 1) ein.

➤ Geben Sie in der SNMP-Shell `isdnlogin <Rufnummer von BinGO!>` ein.

Es erscheint der Login-Prompt. Sie befinden sich auf der SNMP-Shell von **BinGO!**. Fahren Sie fort mit Kapitel 5.2, Seite 107.

5.2 Einloggen

Unabhängig davon, über welchen Weg Sie auf **BinGO!** zugreifen, erscheint immer zunächst die ➤➤ **SNMP-Shell** von **BinGO!** mit dem Login-Prompt:

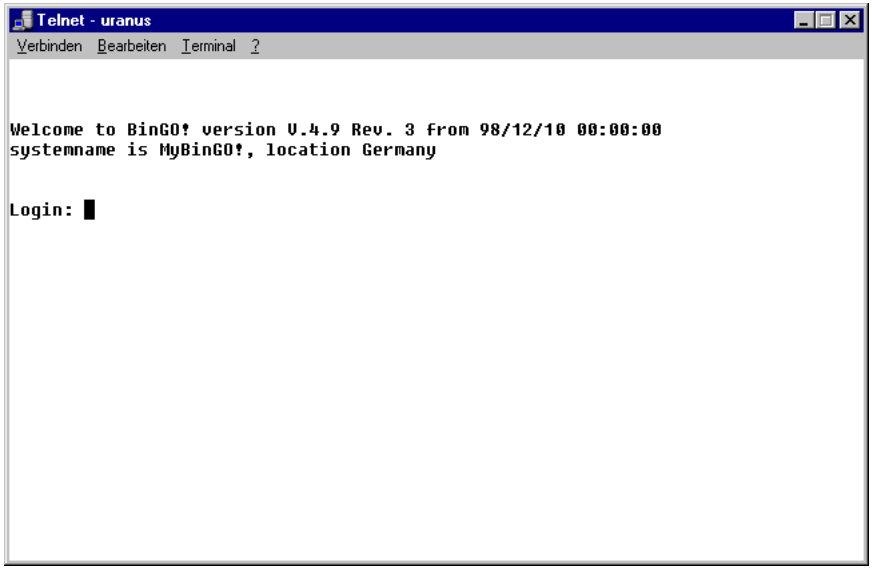


Bild 5-2: Login-Prompt

Um sich einloggen zu können, müssen Sie Benutzername und Paßwort kennen. Im Auslieferungszustand ist **BinGO!** mit folgenden Benutzernamen und Paßwörtern versehen:

Benutzername	Paßwort	Befugnisse
`admin`	bintec	Systemvariablen lesen und ändern, Konfigurationen speichern, Setup Tool benutzen.
`write`	public	Systemvariablen lesen (Änderungen gehen bei Ausschalten von **BinGO!** verloren).
`read`	public	Systemvariablen lesen.
`http`	bintec	HTTP-Statusseite und JAVA Statusmonitor von **BinGO!** aufrufen, Systemvariablen lesen, kein Einloggen.

Tabelle 5-1: Benutzernamen und Paßwörter im Auslieferungszustand

Um also Konfigurationsänderungen vorzunehmen und abzuspeichern, müssen Sie sich mit dem Benutzernamen `admin` einloggen.

Aus Sicherheitsgründen kann man Benutzernamen und Paßwörter nur dann lesen, wenn man sich mit dem Benutzernamen `admin` einloggt. So kann man z. B. mit dem Benutzernamen `read` alle anderen Konfigurationseinstellungen lesen, aber nicht die Zugangsdaten. Es ist also nicht möglich, sich mit `read` einzuloggen, das Paßwort des Benutzers `admin` auszulesen und sich dann anschließend mit `admin` einzuloggen, um Konfigurationsänderungen vorzunehmen.

So loggen Sie sich ein:

- Geben Sie Ihren Benutzernamen ein, z. B. `admin`, und bestätigen Sie mit der **Eingabetaste**.
- Geben Sie Ihr Paßwort ein, z. B. `bintec`, und bestätigen Sie mit der **Eingabetaste**.

  Ihr Router meldet sich mit dem Eingabeprompt, z. B. `brick:>`. Das Einloggen war erfolgreich.

Achtung!

Um unberechtigten Zugriff auf **BinGO!** zu verhindern, sollten Sie gleich als erstes die Paßwörter ändern, falls Sie dies nicht schon bei der Grundkonfiguration mit dem Configuration Wizard getan haben.

➤ Ändern Sie die Paßwörter, wie in Kap. Kapitel 6.1.2, Seite 128 beschrieben

SNMP-Shell schließen

Um die SNMP-Shell nach Beenden der Konfiguration zu verlassen, geben Sie `exit` ein und bestätigen mit der **Eingabetaste**.

5.3 Konfigurationsmöglichkeiten

Bevor Sie mit der Konfiguration loslegen, müssen Sie sich für eine Methode entscheiden. Daher folgt hier zunächst eine Übersicht der verschiedenen Konfigurationsmöglichkeiten und eine Einführung in die Verwendung des Setup Tools. Anhand des Setup Tools beschreibt dieses Handbuch, wie Sie **BinGO!** konfigurieren.

5.3.1 Übersicht

Die Möglichkeiten, **BinGO!** zu konfigurieren:

- Configuration Wizard
- Setup Tool
- ➤➤ **SNMP**-Shell-Kommandos
- ➤➤ **DIME** Browser
- Andere SNMP-Manager

Configuration Wizard

Die Konfiguration mit dem Configuration Wizard haben Sie bereits in Kapitel 3.4, Seite 48 kennengelernt. Sie dient zur schnellen Grundkonfiguration von **BinGO!** und kann genutzt werden, wenn Sie über einen Windows-PC verfügen. Standardkonfigurationen sind in der Regel damit abgedeckt. Wenn Sie aber darüberhinaus noch weitere Einstellungen benötigen, stehen Ihnen die anderen oben genannten Konfigurationsmöglichkeiten zur Verfügung. Sie können zunächst **BinGO!** mit dem Configuration Wizard konfigurieren und anschließend die so erstellte Konfiguration mit einem der anderen Tools erweitern oder ändern. In vielen Fällen wird die Konfiguration mit dem Configuration Wizard aber ausreichend sein!

Setup Tool

Das Setup Tool ist ein menügesteuertes Tool zur Konfiguration und Administration von **BinGO!**. Die Konfiguration mit Setup Tool ist wesentlich einfacher und übersichtlicher als die Konfiguration mit SNMP-Kommandos, allerdings können nicht alle Einstellungen mittels Setup Tool vorgenommen werden. In diesem Handbuch wird neben dem Configuration Wizard ausschließlich das Setup Tool zur Konfiguration beschrieben. Das Setup Tool ist unabhängig vom Betriebssy-

stem auf Ihrem Rechner. Sollte in einzelnen Fällen ein Konfigurationsschritt nur mit Hilfe von SNMP-Kommandos möglich sein, wird die Vorgehensweise zusätzlich beschrieben.

SNMP

➤➤ **SNMP** (Simple Network Management) ist ein ➤➤ **Protokoll**, über das definiert wird, wie Sie auf die Konfigurationseinstellungen zugreifen können. Alle Konfigurationseinstellungen sind in der sog. ➤➤ **MIB** (Management Information Base) in Form von MIB-Tabellen und MIB-Variablen hinterlegt. Auf diese können Sie direkt in der SNMP-Shell zugreifen.

DIME Browser und andere SNMP-Manager

Mit dem ➤➤ **DIME Browser** stellt BinTec Communications AG einen SNMP-Manager für Windows-PCs zur Verfügung. In einer an den Microsoft Explorer angelehnten Oberfläche können Sie damit auf alle MIB-Tabellen und -Variablen von **BinGO!** zugreifen. Über andere SNMP-Manager, wie z. B. SNM, HP-Open View oder Transview, können Sie ebenfalls auf die MIB-Tabellen und MIB-Variablen zugreifen und sie ändern. Für den Umgang mit SNMP-Shell-Kommandos bzw. SNMP-Manager sind allerdings vertiefte Kenntnisse der Struktur und inneren Zusammenhänge von **BinGO!** erforderlich, die Methode ist also für erfahrene Nutzer interessant. In diesem Handbuch wird der Umgang mit MIB-Tabellen und MIB-Variablen nicht erläutert, aber in der Software Reference und MIB Reference.

5.3.2 Setup Tool

Wenn Sie sich auf **BinGO!** eingeloggt haben, können Sie das Setup Tool aufrufen:

➤ Geben Sie nach dem Eingabeprompt `setup` ein und drücken Sie die **Eingabetaste**.

Das Hauptmenü des Setup Tools erscheint.

Hauptmenü

```
BinGO! Setup Tool                                BinTec Communications AG
                                                                MyBinGO!

Licenses                 System

LAN Interface:   CM-BNC/TP, Ethernet
WAN Interface:   CM-1BRI, ISDN S0

WAN Partner
IP      IPX      PPP      ISDN     CAPI

Configuration Management
Monitoring and Debugging

Exit

Press <Ctrl-n>, <Ctrl-p> to scroll through menu items, <Return> to
enter
```

Um das Setup Tool zu nutzen, müssen Sie sich mit dem Benutzernamen `admin` einloggen! Wenn Sie das entsprechende Paßwort nicht kennen, können Sie das Setup Tool nicht aufrufen (siehe Kapitel 5.2, Seite 107).

Das Setup Tool ist einfach zu bedienen. Nach einigen Minuten werden Sie sich gut darin zurechtfinden. Dennoch sollten Sie sich zunächst mit den Möglichkeiten des Setup Tools vertraut machen. Es folgt zunächst eine Einführung in das Setup Tool von **BinGO!**.

Menü-Layout Jedes Setup Tool Menü besteht aus drei Bereichen:

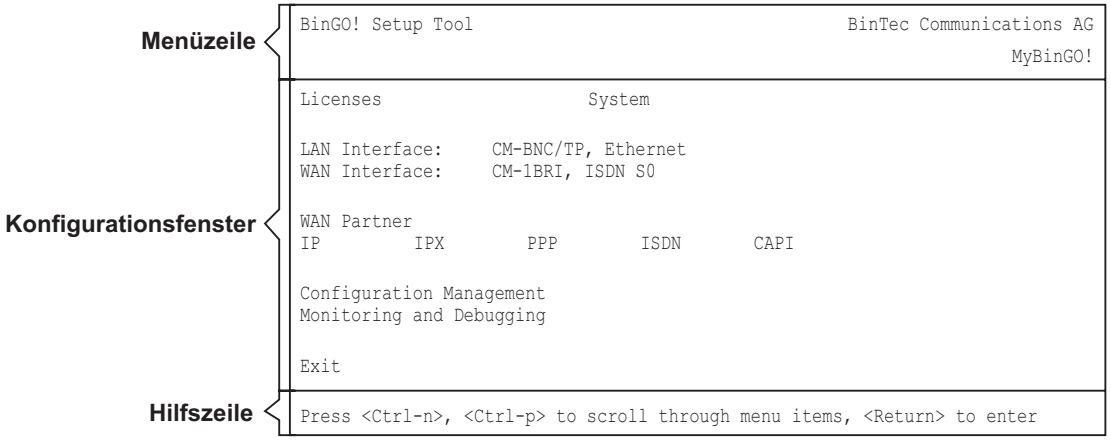


Bild 5-3: Setup Tool Menü-Layout

In der Menüzeile befindet sich eine Navigationshilfe, die anzeigt, in welchem Menü des Setup Tools Sie sich gerade befinden. Zusätzlich wird der Systemname von **BinGO!** angezeigt. Dies ist insbesondere dann hilfreich, wenn Sie mehrere BinTec-Router mit unterschiedlichen Systemnamen einsetzen.

Im Konfigurationsfenster nehmen Sie die eigentlichen Eintragungen vor, und die jeweiligen Einstellungen werden angezeigt. Das Feld, auf dem sich der Cursor zur Zeit befindet, ist invers dargestellt.

Die Hilfszeile gibt an, wie sie sich in dem gerade angezeigten Menü bewegen oder welche Eintragungen Sie ändern können.

Menü-Navigation Um sich im Setup Tool zu bewegen, können Sie die folgenden Tasten bzw. Tastenkombinationen verwenden:

Tastenkombination	Bedeutung
Tabulator	Zum nächsten Feld im Menü springen.
Eingabetaste	Untermenü öffnen oder Kommando (z. B. **SAVE**) aktivieren.
up und **down**	Zum nächsten und vorherigen Feld im Menü springen (funktioniert mit VT 100-Emulation bei Verwendung eines Terminalprogramms).
left und **right**	Vorherige und nachfolgende Werte von Feldern sichtbar machen (funktioniert mit VT 100-Emulation bei Verwendung eines Terminalprogramms).
Esc Esc	Zweimal nacheinander **Esc**: Zum vorherigen Menü zurückkehren. Veränderungen gehen verloren.
Leertaste	Listen-Einträge markieren, die gelöscht werden sollen. Der so markierte Eintrag wird dabei mit D gekennzeichnet. Durch nochmaliges Betätigen der **Leertaste** wird die Markierung wieder entfernt.
Strg - **l**	Anzeige aktualisieren.
Strg - **n**	Zum nächsten Feld im Menü springen.
Strg - **p**	Zum vorherigen Feld im Menü springen.
Strg - **f**	In einer langen Liste, die nicht vollständig angezeigt wird, nach unten blättern. Rechts unten zeigt ein "=" das Ende der Liste bzw. ein "∨" weitere Listeneinträge an.
Strg - **b**	In einer langen Liste, die nicht vollständig angezeigt wird, nach oben blättern. Rechts oben zeigt ein "=" den Anfang der Liste bzw. ein "∧" weitere Listeneinträge an.

Tastenkombination	Bedeutung
Strg - **c**	Setup Tool verlassen.

Tabelle 5-2: Navigation im Setup Tool

Menü-Kommandos

Wenn Sie sich im Setup Tool bewegen, werden Sie feststellen, daß in manchen Menüs spezielle Kommandos, z. B. **DELETE**, **SAVE**, **CANCEL** angeboten werden. Im Folgenden ist die Bedeutung der jeweiligen Kommandos erläutert:

Schaltfläche	Bedeutung
ADD	Einen neuen Punkt zu einer Liste hinzufügen. Ein Untermenü erscheint, wo Sie die gewünschten Einstellungen eintragen.
CANCEL	Alle Änderungen in dem gerade angezeigten Menü löschen.
DELETE	Alle Eintragungen einer Liste löschen, die explizit mit der **Space**-Taste zum Löschen markiert wurden. Die Änderungen werden sofort wirksam.
OK	Die Änderungen im aktuellen Menü bestätigen. Sie werden aber erst wirksam, wenn im nächsten Menü **SAVE** betätigt wird.
SAVE	Alle Eintragungen des aktuellen Menüs im Arbeitsspeicher (Memory) speichern, einschließlich aller Untermenüs. Die Änderungen werden sofort wirksam.
EXIT	Das aktuelle Menü verlassen und zum übergeordneten Menü zurückkehren. Wenn Eintragungen gemacht wurden, gehen diese verloren.

Tabelle 5-3: Schaltflächen im Setup Tool

Listen-Suchfunktion

Einige Menüs des Setup Tool enthalten Listen mit mehreren Einträgen, z. B. das Menü ***WAN PARTNER***, in dem alle ➤➤ **WAN-Partner** aufgelistet sind:

```
BinGO! Setup Tool                                BinTec Communications AG
[WAN]: WAN Partners                                              MyBinGO!


Current WAN Partner Configuration

    Partnername          Protocol             State

    BigBoss              ppp                  dormant      ^
    T_ONLINE             ppp                  dormant      |
    Partner1             ppp                  dormant      |
    Partner2             ppp                  dormant      |
    PROVIDER             ppp                  dormant      =

ADD             DELETE               EXIT

Press <Ctrl-n>, <Ctrl-p> to scroll, <Space> tag/untag DELETE, <Return>
to edit
Search: p
```

Die Listeneinträge sind alphabetisch geordnet nach dem Inhalt des ersten Feldes. Für das Auffinden der Listeneinträge ist eine inkrementelle Suchfunktion eingebaut, die gerade bei sehr langen Listen hilfreich ist.

Gehen Sie folgendermaßen vor:

- Geben Sie den Anfangsbuchstaben des gesuchten Eintrags ein, während der Cursor sich auf einem Listeneintrag befindet. Groß- oder Kleinschreibung spielt dabei keine Rolle.
- Geben Sie weitere Zeichen ein, um die Suche zu verfeinern.
- Editieren Sie die eingegebenen Suchparameter mit der **Backspace**- oder der **Delete**-Taste.

  Der Cursor springt automatisch auf den ersten passenden Eintrag mit den entsprechenden Anfangsbuchstaben.

Die zur Suche eingegebenen Zeichen werden in der Hilfszeile im unteren Bereich des Menüs angezeigt.

Wenn Sie nicht-sichtbare Zeichen eingeben, wird die Suche abgebrochen und evtl. eine Aktion ausgeführt, z. B. bei **Tabulator** oder **Space**.

Falls die Suche nicht funktioniert, achten Sie darauf, daß sich der Cursor auf einem Listen-Element befindet.
Die Suche kann nicht ausgeführt werden, wenn sich der Cursor auf einem Kommando-Feld, z. B. **ADD** oder **DELETE**, befindet.

Beispiel:

Im oben dargestellten Menü ***WAN PARTNER*** liefern die folgenden Eingaben diese Suchergebnisse:

Eingabe	Cursor springt zum Eintrag
p oder P	*Partner1*
pr, Pr, pR, PR	*PROVIDER*
p a r t n e r 2	*Partner1*, nach Eingabe von 2 zu *Partner2*

Tabelle 5-4: Suchergebnisse

Konvention

Damit Sie jederzeit wissen, von welchem Menü des Setup Tools hier im Handbuch gerade die Rede ist bzw. wie Sie dorthin gelangen, gilt folgende Konvention (der Ausgangspunkt ist jeweils das Hauptmenü):

MENÜ ➧ ***UNTERMENÜ*** ➧ ***UNTERMENÜ***

Beispiele:

- "Gehen Sie zum Untermenü Routing, das sich im Menü IP befindet" wird dargestellt als:
  Gehen Sie zu ***IP*** ➧ ***ROUTING***.
- "Gehen Sie zum Untermenü Advanced Settings im Untermenü WAN Numbers. Betätigen Sie dazu im Menü WAN Partner und im Untermenü WAN Numbers jeweils die Schaltfläche ADD, um einen neuen Eintrag zu erzeugen." Dies wird dargestellt als:
  Gehen Sie zu ***WAN PARTNER*** ➧ **ADD** ➧ ***WAN NUMBERS*** ➧ **ADD** ➧ ***ADVANCED SETTINGS***.
- "Gehen Sie zum Untermenü WAN Numbers eines eingetragenen WAN-Partners, um einen bestehenden Eintrag zu verändern. Markieren Sie dazu

im Menü WAN Partner den entsprechenden WAN-Partner und bestätigen Sie mit der Eingabetaste." Dies wird dargestellt als:
Gehen Sie zu ***WAN PARTNER*** ➧ ***EDIT*** ➧ ***WAN NUMBERS***.

Menü-Struktur Die Menü-Struktur des Setup Tools sieht folgendermaßen aus:

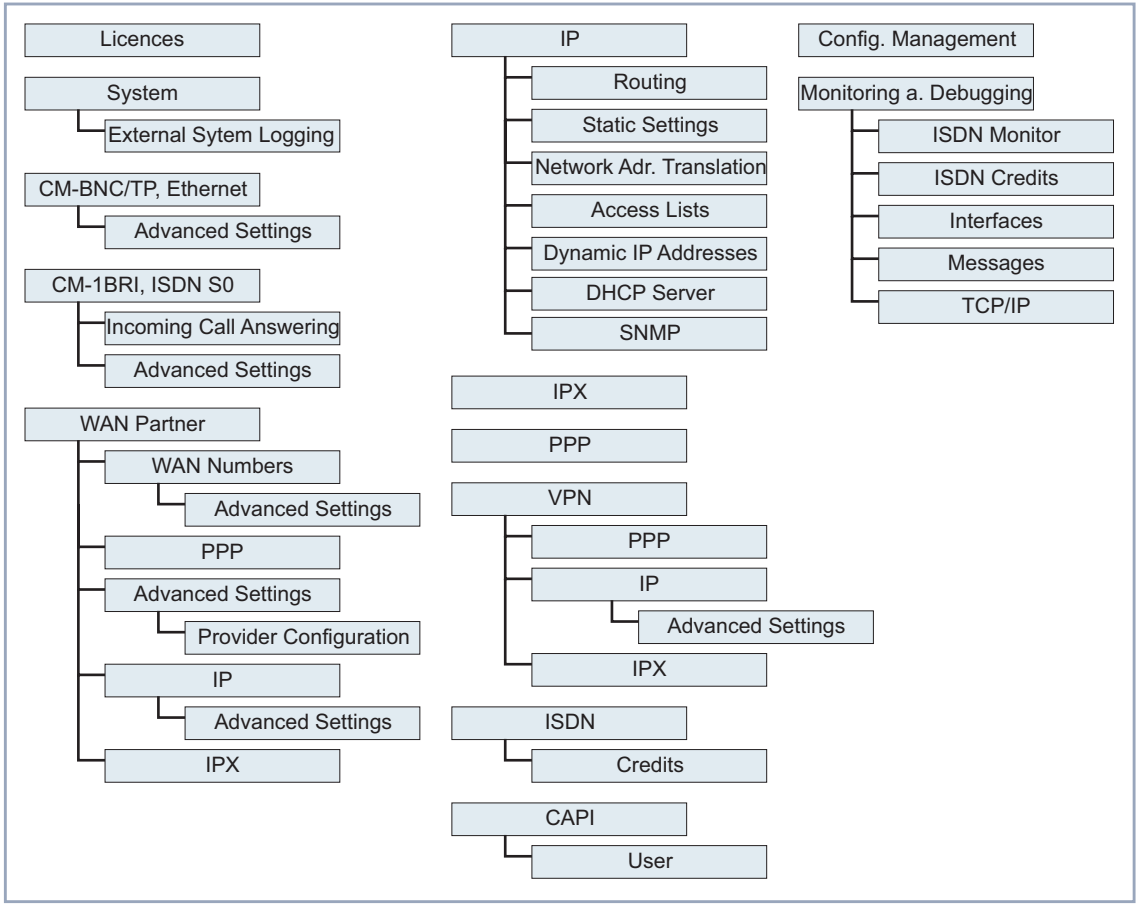


Bild 5-4: Setup Tool Menü Struktur

Bild 5-4, Seite 118 stellt alle auf **BinGO!** zur Verfügung stehenden Menüs des Setup Tools dar. Nicht alle Funktionen stehen auf jedem Router zur Verfügung (z. B. VPN). Um sie nutzen zu können, benötigen Sie eine Zusatzlizenz, die Sie bei BinTec Communications GmbH erwerben können. Wenn Sie die erforderli-

che Lizenz aktivieren, erkennt dies **BinGO!** und zeigt die entsprechenden Menüs an (Lizenz eintragen siehe Kapitel 6.1.1, Seite 126).

Überblick Um die Orientierung bei der Konfiguration zu erleichtern, werden die Menüs kurz erläutert. Die genaue Beschreibung der einzelnen Konfigurationsschritte, die für die gewünschten Einstellungen erforderlich sind, erfolgt dann in den weiteren Kapiteln.

Menü	Funktion
LICENSES	In diesem Menü tragen Sie die Lizenzinformationen ein, die auf der mitgelieferten Lizenzkarte vermerkt sind. Hier aktivieren Sie auch die Zusatzlizenzen.
SYSTEM	In diesem Menü tragen Sie die grundlegenden Systemeinstellungen von **BinGO!** ein, wie z. B. Systemname und Paßwörter.
CM-BNC/TP, ETHERNET	In diesem Menü konfigurieren Sie die ➤➤ **LAN**-Schnittstelle von **BinGO!**. Hier tragen Sie z. B. die IP-Adresse und Netzmaske von **BinGO!** ein.
CM-1BRI, ISDN S0	In diesem Menü konfigurieren Sie die ➤➤ **WAN**-Schnittstelle von **BinGO!**. Hier tragen Sie z. B. ein, an welcher Art von ISDN-Anschluß **BinGO!** angeschlossen ist. In dem Untermenü ***WAN INTERFACE*** ➧ ***INCOMING CALL ANSWERING*** teilen Sie die zur Verfügung stehenden ISDN-Rufnummern den gewünschten Diensten (z. B. PPP-Routing, ➤➤ **CAPI**, ➤➤ **ISDN-Login**) zu.
WAN PARTNER	In diesem Menü definieren Sie alle WAN-Partner, z. B. Ihren ➤➤ **Internet** Service Provider (➤➤ **ISP**). Sie können bis zu 4 WAN-Partner anlegen, mit einer Zusatzlizenz können Sie die Beschränkung auf 4 WAN-Partner aufheben. Alle eingetragenen WAN-Partner werden in einer Liste angezeigt, die den Partnernamen, das verwendete Protokoll und den aktuellen Status enthält.

Menü	Funktion
IP	In diesem Menü tragen Sie die Einstellungen ein, die das ➤➤ **IP**-Protokoll betreffen. Es besteht aus mehreren Untermenüs: ***IP*** ➧ ***ROUTING*** enthält die IP-Routingtabelle von **BinGO!**. Hier tragen Sie Routen zu Ihren Partnern ein (z. B. Default-Routen, Netzwerk-Routen), damit **BinGO!** alle ➤➤ **Datenpakete** an die richtigen Adressen weiterleitet. In ***IP*** ➧ ***STATIC SETTINGS*** trage Sie einige wichtige Einstellungen ein, z. B. den Domain Name von **BinGO!**, die IP-Adressen zusätzlicher ➤➤ **Server** (z. B. Domain Name Server), Angaben über die Systemzeit. In ***IP*** ➧ ***NETWORK ADDRESS TRANSLATION*** konfigurieren Sie die Schnittstellen zu den Partnern, für die Sie die Funktion Network Address Translation (➤➤ **NAT**) nutzen wollen. In ***IP*** ➧ ***ACCESS LISTS*** definieren Sie ➤➤ **Filter**, um den Zugang von bzw. zu den verschiedenen Hosts in angeschlossenen Netzwerken zu erlauben oder zu sperren. So können Sie verhindern, daß **BinGO!** ungewollt Verbindungen zum ISDN aufbaut. In ***IP*** ➧ ***DYNAMIC IP ADDRESSES*** können Sie einen Pool von IP-Adressen einrichten, die **BinGO!** als dynamischer IP Address Server an WAN-Partner vergibt, die sich einwählen. In ***IP*** ➧ ***DHCP SERVER*** konfigurieren Sie **BinGO!** als ➤➤ **DHCP**-Server. Als DHCP-Server teilt **BinGO!** den Hosts im LAN deren IP-Adressen dynamisch zu. In ***IP*** ➧ ***SNMP*** können Sie die grundlegenden ➤➤ **SNMP**-Einstellungen ändern.
IPX	In diesem Menü nehmen Sie die Eintragungen vor, die das IPX-Protokoll betreffen. ➤➤ **IPX** wird vor allem in Novell-Netzwerken verwendet.

Menü	Funktion
PPP	Enthält allgemeingültige ➤➤ **PPP**-Einstellungen, z. B. Authentication Protocol, die sich nicht nur auf einzelne WAN-Partner beziehen. Mit diesen Einstellungen führt der Router mit eingehenden Rufen eine Authentisierungsverhandlung aus, wenn er die Calling Line Number nicht identifizieren kann (z. B. weil der Anruf über eine analoge Leitung eingeht, die die Calling Line Number nicht transportiert).
VPN	In diesem Menü nehmen Sie die nötigen Einstellungen für Virtual Private Networking (VPN) vor. Es erscheint nur, wenn Sie eine dafür gültige Lizenz eingetragen haben. Um die Funktion nutzen zu können, brauchen Sie einen VPN-Server von Security Dynamics. Die Lizenz können Sie optional erwerben. Detaillierte Erklärungen und Hinweise zur Konfiguration finden Sie in der Extended Feature Reference.
ISDN	In diesem Menü verwalten Sie das Taschengeldkonto (Credits Based Accounting System) von **BinGO!**.
CAPI	Enthält die Einstellungen für das ➤➤ **CAPI** User Concept von BinTec. Damit können Sie an Nutzer der CAPI-Anwendungen von **BinGO!** Benutzernamen und Paßwörter vergeben. So stellen Sie sicher, daß nur autorisierte Nutzer eingehende Rufe empfangen und ausgehende Verbindungen via CAPI aufbauen können.
CONFIGURATION MANAGEMENT	In diesem Menü verwalten Sie die Konfigurationsdateien von **BinGO!**. Sie speichern Sie z. B. lokal auf **BinGO!** oder aber auf Ihrem Rechner ab.
MONITORING AND DEBUGGING	Enthält Untermenüs, die das Auffinden von Problemen in Ihrem Netzwerk und das Überwachen von Aktivitäten, z. B. an der WAN-Schnittstelle von **BinGO!**, ermöglichen.
EXIT	Mit **Exit** verlassen Sie das Setup Tool. Mit **Exit** ➧ **Save as boot configuration and exit** speichern Sie die Konfigurationsdatei im Flash-Speicher, nach einem Restart von **BinGO!** wird diese Datei geladen. Mit **Exit** ➧ **Exit without saving** gehen seit dem letzten Hochfahren von **BinGO!** gemachte Änderungen verloren.

Tabelle 5-5: Menüs im Setup Tool

5 Ein Draht zu BinGO!

6 Grundkonfiguration mit Setup Tool

Die Grundkonfiguration von **BinGO!** mit dem ➤➤ **Setup Tool** beinhaltet die gleichen Themen wie die Konfiguration mit dem Configuration Wizard in Kapitel 3.4, Seite 48. Allerdings ist das Setup Tool unabhängig vom Betriebssystem und Sie können zusätzlich weitere Einstellungen vornehmen.

Grundkonfiguration

Die Grundkonfiguration von **BinGO!** umfaßt:

- Die grundlegenden ➤➤ **Router**einstellungen
- Das Einrichten von ➤➤ **WAN**-Partnern
  - für Internetzugang
  - für LAN-LAN-Kopplung (z. B. Firmennetzanbindung)
- Das Sichern der Konfigurationsdatei

Die grundlegenden Routereinstellungen sind für das Funktionieren von **BinGO!** unbedingt erforderlich. Den Internetzugang und die Firmennetzanbindung können Sie je nach Bedarf gleich einrichten oder später hinzufügen.

Bestehende Konfiguration erweitern

Wenn Sie keine Grundkonfiguration durchführen, aber Ihre bestehende Konfiguration ändern wollen, dann finden Sie in diesem Kapitel ebenfalls nützliche Hinweise, z. B.

- wie Sie einen weiteren ➤➤ **WAN-Partner** hinzufügen.
- wie Sie die Paßwörter ändern.
- wie Sie eine Zusatzlizenz eintragen.
- wie Sie das Verteilen der eingehenden Anrufe (Incoming Call Answering) organisieren.
- wie Sie **BinGO!** als ➤➤ **DHCP**-Server einrichten.
- wie Sie einen einfachen ➤➤ **NetBIOS**-Filter definieren.
- wie Sie Routing-Einträge erstellen.

Wie Sie weitere Konfigurationschritte nach Abschluß der Grundkonfiguration durchführen, finden Sie in Kapitel 7, Seite 189.

Wie Sie Sicherheitsmechanismen gemäß SAFERNET einrichten, finden Sie in Kapitel 8, Seite 235.

6.1 Grundlegende Routereinstellungen

Das Einrichten der grundlegenden Routereinstellungen betrifft nur **BinGO!** und Ihr lokales Netzwerk. In Bild 6-1, Seite 125 ist der relevante Ausschnitt aus Bild 6-2, Seite 137 abgebildet. Dort sind beispielhaft Namen, ➤➤ **IP-Adressen**, Rufnummern, etc. angegeben. Wenn Sie ein neues lokales Netzwerk (LAN) zusammen mit **BinGO!** einrichten und keine IP-Adressen zugeteilt bekommen haben (z. B. von Ihrem System-Administrator in der Firmenzentrale), übernehmen Sie als IP-Adressen einfach die Beispielwerte. Natürlich können Sie auch alle anderen für Sie sinnvollen Werte verwenden.

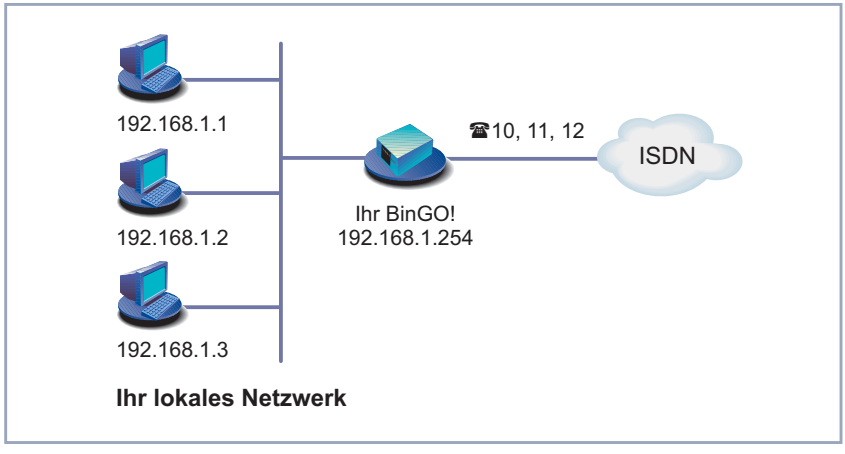


Bild 6-1: Grundlegende Routereinstellungen

Folgende Schritte sind erforderlich:

- Lizenz eintragen
- Systemdaten (z. B. Paßwörter) eintragen
- LAN-Schnittstelle konfigurieren
- ➤➤ **WAN-Schnittstelle** konfigurieren
- **BinGO!** als DHCP-➤➤ **Server** einrichten (optional)
- ➤➤ **Filter** setzen (optional, ausführlich in Kapitel 8.2.8, Seite 258)

Los geht's:

6.1.1 Lizenz eintragen

Lizenzkarte

Nachdem Sie sich wie in Kapitel 5.2, Seite 107 beschrieben auf **BinGO!** mit dem Benutzernamen `admin` eingeloggt und das Setup Tool mit `setup` aufgerufen haben, tragen Sie zunächst die Lizenzinformationen ein. Diese sind auf der mitgelieferten Lizenzkarte vermerkt. Damit schalten Sie die Funktionen von **BinGO!** frei.

➤ Gehen Sie zu ***LICENSES:***

```
BinGO! Setup Tool                                BinTec Communications AG
[LICENSE]: Licenses                                              MyBinGO!

Available Licenses:

IP (builtin), EXTENDLAN (not_valid), TUNNEL (not_valid), STAC (valid)
CAPI (valid), IPX (valid)

Serialnumber         Mask         Key          State
101546               51           88PNUPZ      ok


ADD                        DELETE                          EXIT

Press <Ctrl-n>,<Ctrl-p> to scroll,<Space> tag/untag DELETE,<Return> to
edit
```

Unter *Available Licenses* sind die auf **BinGO!** verfügbaren Subsysteme und deren Status (*builtin* - immer verfügbar, *valid* - freigeschaltet, *not_valid* - nicht freigeschaltet) aufgelistet.

Darunter ist die eingetragene Lizenz (*Serialnumber*, *Mask*, *Key*) abgebildet.

Wenn Sie noch keine Lizenz eingetragen haben, ist die Subsystem-Liste fast leer. Nur *IP*, also ➤➤ **IP**-Routing, ist verfügbar (*builtin*).

Subsysteme Folgende Subsysteme stehen prinzipiell auf **BinGO!** zur Verfügung:

Subsysteme	Bedeutung
IP	IP-Routing.
EXTENDLAN	Unbegrenzte Anzahl an LAN-Partnern (nur mit Zusatzlizenz).
TUNNEL	Virtual Private Networking VPN (nur mit Zusatzlizenz).
STAC	➤➤ **STAC**-➤➤ **Datenkompression**.
CAPI	➤➤ **Remote-CAPI**-Schnittstelle, ermöglicht Kommunikationsanwendungen auf Ihrem Rechner, z. B. Faxe versenden und empfangen.
IPX	➤➤ **IPX**-Routing.

Tabelle 6-1: Subsysteme

ToDo Gehen Sie folgendermaßen vor, um Ihre Lizenz einzutragen:

- ➤ Fügen Sie einen neuen Eintrag mit **ADD** hinzu.
  Ein weiteres Menüfenster erscheint.
- ➤ Geben Sie *Serial Number* ein.
- ➤ Geben Sie *Mask* ein.
- ➤ Geben Sie *Key* ein.
- ➤ Bestätigen Sie mit **SAVE.**
  Sie befinden sich wieder im Menü ***LICENSES***. Die mit Ihrer Lizenz freigeschalteten Subsysteme sind aufgelistet. Ihre Lizenz ist eingetragen, sie wird mit dem Status *ok* angezeigt.

Wenn als Status *not ok* angezeigt wird, haben Sie sich wahrscheinlich vertippt.

- ➤ Versuchen Sie es erneut.

6.1.2 Systemdaten eintragen

Paßwörter, Systemname, ...

Tragen Sie als nächstes die grundlegenden Systemdaten zur Identifikation von **BinGO!** ein.

➤ Gehen Sie zu ***SYSTEM:***

```
BinGO! Setup Tool                                BinTec Communications AG
[SYSTEM]: Change System Parameters                                MyBinGO!

System Name                                      MyBinGO!
Local PPP ID (default)                           LittleIndian
Location                                         3rd floor
Contact                                          admin@BigBoss.com

admin Login Password/SNMP Community              secret
read Login Password/SNMP Community               secret1
write Login Password/SNMP Community              secret2

HTTP Server Password                             secret3
Syslog output on serial console                  no
Message level for the syslog table               info
Maximum Number of Syslog Entries                 20

External System Logging>

            SAVE                                     CANCEL

Enter string, max length = 34 chars
```

Folgende Teile des Menüs sind für diesen Konfigurationsschritt interessant:

Feld	Bedeutung
System Name	Definiert den Systemnamen von **BinGO!**, wird auch als PPP-Host-Name benutzt. Erscheint beim Einloggen auf **BinGO!** als Eingabe-Prompt. Wenn kein Systemname gesetzt ist, erscheint beim Einloggen mit dem Benutzernamen `admin` ein Warnhinweis.
Local PPP ID	Diese Eintragung ist zur Identifizierung von **BinGO!** nötig, wenn eine nicht-partnerspezifische ➤➤ **PPP-Authentisierung** (z. B. ➤➤ **PAP** oder ➤➤ **CHAP**) durchgeführt wird (siehe Kapitel 7.1.4, Seite 198).
Location	(optional) Gibt an, wo sich **BinGO!** befindet.
Contact	(optional) Gibt die zuständige Kontaktperson an. Wenn die Person von der HTTP-Statusseite von **BinGO!** aus erreichbar sein soll, muß hier eine gültige E-Mail-Adresse eingetragen werden.

Feld	Bedeutung
admin Login Password	Paßwort für Benutzername admin.
read Login Password	Paßwort für Benutzername read.
write Login Password	Paßwort für Benutzername write.
HTTP Server Password	Paßwort für die HTTP-Statusseite von **BinGO!**.

Tabelle 6-2: ***SYSTEM***

Achtung!

Alle BinTec-Router werden mit gleichem Benutzernamen und Paßwort ausgeliefert. Sie sind daher nicht gegen einen unautorisierten Zugriff geschützt, solange die Paßwörter nicht geändert wurden.

- Ändern sie unbedingt die Paßwörter, um unberechtigten Zugriff auf **BinGO!** zu verhindern.

Die Befugnisse der möglichen Benutzernamen und Paßwörter finden Sie in Kapitel 5.2, Seite 107.

ToDo Gehen Sie folgendermaßen vor, um die relevanten Systemdaten einzutragen:

- Geben Sie *System Name* von **BinGO!** ein, z. B. ***MyBinGO!***.
- Geben Sie *Local PPP ID* ein. Der Eintrag kann mit *System Name* übereinstimmen.
- Geben Sie *Location* ein, z. B. ***Europe***.
- Geben Sie *Contact* ein, z. B. ***SysAdmin***.
- Geben Sie *admin Login Password* ein.
- Geben Sie *read Login Password* ein.
- Geben Sie *write Login Password* ein.
- Geben Sie *HTTP Server Password* ein.
- Bestätigen Sie mit **SAVE**.

  Sie befinden sich wieder im Hauptmenü, die Eintragungen sind gespeichert.

6.1.3 LAN-Schnittstelle konfigurieren

➤➤ **IP-Adresse,**
➤➤ **Netzmaske,**
➤➤ **Encapsulation**

Konfigurieren Sie als nächstes die LAN-Schnittstelle von **BinGO!**. Die LAN-Schnittstelle ist die physikalische Schnittstelle zum lokalen Netzwerk. Im folgenden Menü geben Sie Ihrem Router die Adresse, unter der er im LAN zu erreichen ist. Solange Ihr Router diese Eintragungen nicht hat, kann er von anderen Hosts nicht als Teil des LANs erkannt werden.

Möglicherweise haben Sie **BinGO!** schon vor der Grundkonfiguration seine IP-Adresse und Netzmaske zugewiesen, z. B. mit Hilfe des ➤➤ **BootP**-Servers der ➤➤ **DIME Tools**. Überprüfen Sie trotzdem die Eintragungen im folgenden Menü.

➤ Gehen Sie zu ***CM-BNC/TP, ETHERNET:***

```
BinGO! Setup Tool                              BinTec Communications AG
[LAN]: Configure Ethernet Interface                            MyBinGO!


IP-Configuration
local IP-Number          192.168.1.254
local Netmask            255.255.255.0
Encapsulation            Ethernet II

IPX-Configuration
local IPX-Netnumber      0
Encapsulation            none

Advanced Settings>

            SAVE                              CANCEL

Enter IP address (a.b.c.d or resolvable hostname)
```

In dem Menü sind Einträge für IP- und ➤➤ **IPX**-Konfiguration möglich. In diesem Kapitel wird nur die Konfiguration von ➤➤ **IP** erläutert. Belassen Sie die unter *IPX-Configuration* voreingestellten Werte.

Wenn Sie das ➤➤ **Protokoll** IPX verwenden, finden Sie Erläuterungen zur Konfiguration der LAN-Schnittstelle für IPX in Kapitel 7.4, Seite 227.

Folgende Teile des Menüs sind für diesen Konfigurationsschritt interessant:

Feld	Bedeutung
local IP-Number	IP-Adresse von **BinGO!** im LAN.
local Netmask	Netzmaske des Netzwerkes, in dem sich **BinGO!** befindet.
Encapsulation	Definiert, welche Art von Header den IP-Paketen, die über diese LAN-Schnittstelle laufen, hinzugefügt wird. Mögliche Werte: ■ *Ethernet II* (entspricht IEEE 802.3) ■ *Ethernet SNAP* I. A. können Sie den voreingestellten Wert *Ethernet II* belassen. Mit *Ethernet II* heißt die LAN-Schnittstelle en1, mit *Ethernet SNAP* en1-snap.

Tabelle 6-3: ***CM-BNC/TP, ETHERNET***

ToDo Gehen Sie folgendermaßen vor, um die LAN-Schnittstelle von **BinGO!** zu konfigurieren:

- Geben Sie *local IP-Number* von **BinGO!** ein, z. B. ***192.168.1.254***.
- Geben Sie *local Netmask* ein, z. B. ***255.255.255.0***.
- Wählen Sie *Encapsulation* aus, z. B. ***Ethernet II***.
- Bestätigen Sie mit **SAVE**.

  Sie befinden sich wieder im Hauptmenü, die Eintragungen sind gespeichert.

6.1.4 WAN-Schnittstelle konfigurieren

Schnittstelle zum ISDN

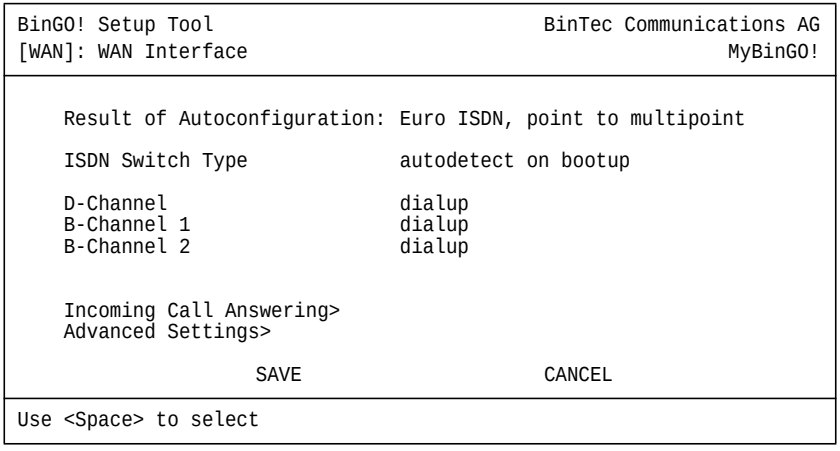
Konfigurieren Sie als nächstes die ➤➤ **WAN-Schnittstelle** von **BinGO!**. Die WAN-Schnittstelle ist die physikalische Schnittstelle zum ➤➤ **ISDN**. Um sie zu konfigurieren, müssen Sie zwei Schritte durchführen:

- Einstellungen Ihres ISDN-Anschlusses eintragen:
  Hier tragen Sie die wichtigsten Parameter Ihres ISDN-Anschlusses ein.
- Incoming Call Answering konfigurieren:
  Hier teilen Sie Ihrem ➤➤ **Router** mit, wie er auf eingehende Rufe aus dem WAN reagieren soll.

Autokonfiguration, ISDN Switch Type, ...

Machen Sie zunächst die Einstellungen für Ihren ISDN-Anschluß.

➤ Gehen Sie zu ***CM-1BRI, ISDN S0:***



Das Menü hat folgende Felder:

Feld	Bedeutung
Result of Autoconfiguration	Status der ISDN-Autokonfiguration. Die automatische ➤➤ **D-Kanal**-Erkennung läuft, bis eine Einstellung gefunden wird bzw. bis das ISDN-Protokoll unter ISDN switch type manuell eingegeben ist.
ISDN Switch Type	Definiert das ISDN-➤➤ **Protokoll**, das Ihnen Ihre Telefongesellschaft zur Verfügung stellt. Folgende Protokolle werden unterstützt: ■ *Euro ISDN* ■ *1TR6* ■ *National ISDN 1 AT&T NI1, EWSD NI1* ■ *AT&T 5ESS Custom ISDN* ■ *National ISDN 1 Northern Telecom DMS100* ■ *Japan NTT INS64*

Feld	Bedeutung
D-Channel	Einstellung des D-Kanals. Der Wert dialup kann nicht verändert werden.
B-Channel 1	Einstellung des ersten ➤➤ **B-Kanals**. Mögliche Werte: ■ *dialup* (Standardwert) ■ *not used*
B-Channel 2	Einstellung des zweiten B-Kanals. Mögliche Werte: ■ *dialup* (Standardwert) ■ *not used*
SPID B-Channel 1+2	Erforderlich für AT&T-Protokolle. Setzt den SPID (Service Profile Identifier) für beide B-Kanäle.
SPID B-Channel 1	Erforderlich für National ISDN 1 Northern Telecom-Protokolle. Setzt den SPID (Service Profile Identifier) für den ersten B-Kanal.
SPID B-Channel 2	Erforderlich für National ISDN 1 Northern Telecom-Protokolle. Setzt den SPID (Service Profile Identifier) für den zweiten B-Kanal.
Incoming Call Answering B1	Erforderlich für National ISDN 1 Northern Telecom-Protokoll. Die Einstellungen für Incoming Call Answering müssen für jeden B-Kanal einzeln eingestellt werden.
Incoming Call Answering B2	Erforderlich für National ISDN 1 Northern Telecom-Protokoll. Die Einstellungen für Incoming Call Answering müssen für jeden B-Kanal einzeln eingestellt werden.

Tabelle 6-4: ***CM-1BRI, ISDN S0***

ToDo Gehen Sie folgendermaßen vor, um die Einstellungen Ihres ISDN-Anschlusses einzutragen:

➤ Wählen Sie *ISDN Switch Type* aus: *autodetect on bootup*.

Mit dieser Einstellung nutzt **BinGO!** die automatische D-Kanal-Erkennung. Unter *Result of Autoconfiguration* erscheint *running*, solange die D-Kanal-Erkennung läuft. Danach wird die gefundene Einstellung angezeigt, z. B. *Euro ISDN, point to multipoint*.

Wenn das ISDN-Protokoll nicht erkannt wird, können Sie es unter *ISDN Switch Type* manuell eingeben. Die automatische D-Kanal-Erkennung ist dann ausgeschaltet.

Bei falsch eingestelltem ISDN-Protokoll kann kein ISDN-Verbindungsaufbau erfolgen!

➤ Wählen Sie *B-Channel 1* aus: *dialup*.

➤ Wählen Sie B-Channel 2 aus: *dialup*.

➤ Bestätigen Sie mit **SAVE**.

Sie befinden sich wieder im Hauptmenü. Die Eintragungen sind gespeichert.

Incoming Call Answering Als nächstes müssen Sie Ihrem Router mitteilen, wie er auf eingehende Rufe aus dem ISDN reagieren soll. Entsprechend den Einstellungen in den folgenden Menüs verteilt **BinGO!** die eingehenden Rufe auf die internen Dienste.

BinGO! unterstützt die Dienste:

- PPP (Routing):
  Der Dienst ➤➤ **PPP** ist der allgemeine Routing-Dienst von **BinGO!**. Damit werden eingehenden Daten-Rufen von WAN-Partnern ➤➤ **Wählverbindungen** mit Ihrem ➤➤ **LAN** ermöglicht. So können Sie es Partnern außerhalb Ihres lokalen Netzwerkes ermöglichen, auf Hosts in Ihrem LAN zuzugreifen.

- ISDN-Login:
  Der Dienst ➤➤ **ISDN-Login** ermöglicht eingehenden Daten-Rufen Zugang zur ➤➤ **SNMP-Shell** von **BinGO!**. So kann **BinGO!** aus der Ferne konfiguriert und gewartet werden.

- CAPI:
  Der Dienst ➤➤ **CAPI** ermöglicht eingehenden Daten- und Sprach-Rufen eine Verbindung mit Kommunikationsanwendungen auf Hosts im LAN, die auf die ➤➤ **Remote-CAPI**-Schnittstelle von **BinGO!** zugreifen. So können beispielsweise mit **BinGO!** verbundene Hosts Faxe empfangen.

Wenn ein Ruf eingeht, überprüft **BinGO!** zunächst die Called Party Number (CPN) und die Art des Anrufs (Daten- oder Sprach-Ruf). CPN ist die Rufnummer, die der Partner gewählt hat, um **BinGO!** zu erreichen. Anschließend wird der Ruf an den passenden Dienst weitergeleitet (siehe auch Bild 6-2, Seite 137).

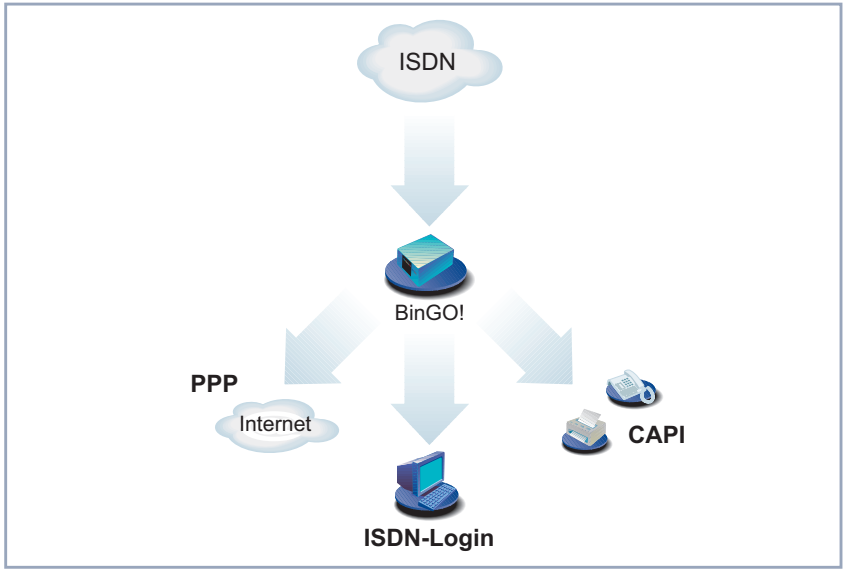


Bild 6-2: Verteilung der eingehenden Rufe auf Dienste

Wenn Ihr ISDN-Anschluß über drei Rufnummern verfügt, könnte eine sinnvolle Aufteilung folgendermaßen aussehen:

Called Party Number	Datendienste	Sprachdienste
10	PPP (Routing)	
11	CAPI	CAPI
12	ISDN-Login	

Tabelle 6-5: Verteilung der Rufnummern auf Dienste

Wenn Sie im folgenden Menü keine Eintragungen vornehmen, wird jeder eingehende Ruf von dem Dienst ISDN-Login angenommen. Um dies zu vermeiden, machen Sie hier auf jeden Fall die erforderlichen Eintragungen.

Sobald Sie in diesem Menü einen oder mehrere Einträge erstellt haben, werden die passenden eingehenden Rufe an die entsprechenden Dienste zugeteilt.

Alle eingehenden Rufe, die nicht zu einem Eintrag passen, werden an den Dienst CAPI weitergeleitet.

Machen Sie nun die Eintragungen für Incoming Call Answering:

➤ Gehen Sie zu ***CM-1BRI, ISDN S0*** ➧ ***INCOMING CALL ANSWERING:***

```
BinGO! Setup Tool                              BinTec Communications AG
[WAN][INCOMING]: Incoming Call Answering                       MyBinGO!


Item                          Number      Mode            Username
CAPI 1.1 EAZ 1 Mapping        11          right to left
CAPI 1.1 EAZ 1 Mapping        11          right to left
ISDN Login                    12          right to left
PPP (routing)                 10          right to left


    ADD                 DELETE              EXIT

Press <Ctrl-n>,<Ctrl-p> to scroll,<Space> tag/untag DELETE,<Return> to
edit
```

In diesem Menü sind die Zuteilungen der Dienste zu den Rufnummern aufgelistet.

Gehen Sie folgendermaßen vor, um Eintragungen in die Liste vorzunehmen:

- Fügen Sie mit **ADD** einen neuen Eintrag hinzu oder wählen Sie einen bestehenden Eintrag aus. Bestätigen Sie mit der **Eingabetaste**, um den Eintrag zu ändern.

  Ein weiteres Menüfenster erscheint:

```
BinGO! Setup Tool                              BinTec Communications AG
[WAN][INCOMING][ADD]:Incoming Call Answering                   MyBinGO!


    Item                    PPP (routing)
    Number                  10
    Mode                    right to left
    Username
    Bearer                  data

                SAVE                    CANCEL

Use <Space> to select
```

Das Menü enthält folgende Felder:

Feld	Bedeutung
Item	Dienst, dem ein Ruf auf die untenstehende *Number* zugewiesen werden soll.
Number	Rufnummer, unter der der oben eingetragene Dienst (*Item*) erreicht werden kann.
Mode	Modus, mit dem **BinGO!** den Ziffernvergleich von *Number* mit der Called Party Number des eingehenden Rufes durchführt: ■ *right to left* (Standardwert) ■ *left to right (DDI):* Immer auswählen, wenn **BinGO!** mit einem Point-to-Point-Anschluß (Anlagenanschluß) verbunden ist.
Username	CAPI-Benutzername. Nur erforderlich, wenn Sie das CAPI User Concept nutzen wollen (siehe Kapitel 7.1.2, Seite 192).
Bearer	Art des eingehenden Rufes. Mögliche Werte: ■ *data:* Daten-Ruf ■ *voice:* Sprach-Ruf ■ *any:* sowohl Daten- als auch Sprach-Ruf

Tabelle 6-6: ***CM-1BRI, ISDN S0*** ➧ ***INCOMING CALL ANSWERING*** ➧ **ADD**

Das Feld *Item* enthält folgende Auswahlmöglichkeiten:

Mögliche Werte	Bedeutung
PPP (routing)	Standardeinstellung für ➤➤ **PPP**-Routing. Zutreffend auch für die unten genannten PPP-Verbindungen.
ISDN Login	Ermöglicht Einloggen mit ➤➤ **isdnlogin**.
PPP 64k	Ermöglicht 64 kbps PPP-Datenverbindungen.
PPP 56k	Ermöglicht 56 kbps PPP-Datenverbindungen.
PPP Modem	Auf **BinGO!** nicht verfügbar.
PPP DOVB	Data transmission Over Voice Bearer – nützlich z. B. in den USA, wo Sprachverbindungen manchmal billiger sind als Datenverbindungen.
PPP V.110 (1200...38400)	Ermöglicht PPP-Verbindungen mit V.110 mit Bit-Raten von 1200 bps, 2400 bps,..., 38400 bps.
Pots	Auf **BinGO!** nicht verfügbar.
PPP Modem Profile 1...8	Auf **BinGO!** nicht verfügbar.
CAPI 1.1 EAZ 0...9 Mapping	Ermöglicht Verbindungen mit Remote-CAPI-Applikationen. Nur erforderlich für CAPI 1.1-Applikationen.
X.25 PAD	Auf **BinGO!** nicht verfügbar.

Tabelle 6-7: *Item*

ToDo Machen Sie folgende Eintragungen:

- Wählen Sie *Item* aus, z. B. ***PPP (routing)***.
- Geben Sie *Number* ein, z. B. ***10***.
- Wählen Sie *Mode* aus, z. B. ***right to left***.
- Wählen Sie *Bearer* aus, z. B. ***data***.

➤ Bestätigen Sie mit **SAVE**.

Sie befinden sich wieder im Menü ***CM-1BRI, ISDN S0*** ➧ ***INCOMING CALL ANSWERING***. Die Eintragungen sind gespeichert und werden in der Liste angezeigt.

Sie haben damit einer Ihrer Rufnummern (***10***) einen möglichen Dienst (***PPP (routing)***) zugeordnet. D. h. wenn ein Daten-Ruf an die Called Party Number 10 eingeht, wird er an den Dienst PPP (routing) weitergeleitet.

Da **BinGO!** alle eingehenden Rufe, die zu keinem Eintrag in diesem Menü passen, an den Dienst ➤➤ **CAPI** weiterleitet, ist es nicht unbedingt erforderlich, CAPI einzutragen!. (Außer für CAPI 1.1-Anwendungen.)

➤ Wiederholen Sie diese Schritte so oft, bis Sie allen Rufnummern die Dienste zugeordnet haben, die unter diesen Rufnummern erreichbar sein sollen.

Damit haben Sie Incoming Call Answering konfiguriert, **BinGO!** verteilt die eingehenden Rufe an die internen Dienste.

Achten Sie darauf, unter *Number* die richtige Nummer, d. h. die Nummer, die auch wirklich bei **BinGO!** ankommt, einzutragen! Wenn **BinGO!** z. B. an einer ➤➤ **TK-Anlage** angeschlossen ist, kommt nur die Nebenstellennummer bei **BinGO!** an.

Wenn Sie sich nicht sicher sind, welche Nummer bei **BinGO!** wirklich ankommt, gehen Sie folgendermaßen vor:

➤ Rufen Sie mit einem herkömmlichen Telefon **BinGO!** mit einer seiner Rufnummern an.

➤ Gehen Sie zu ***MONITORING AND DEBUGGING*** ➧ ***ISDN MONITOR***.

Im Menü können Sie jetzt den eingehenden Ruf sehen.

➤ Setzen Sie den Cursor auf den Ruf und geben Sie d (für details) ein.

Unter *Local Number* sehen Sie den Anteil der Rufnummer, die bei **BinGO!** ankommt.

➤ Geben Sie diesen Anteil der Rufnummer in ***CM-1BRI, ISDN S0*** ➧ ***INCOMING CALL ANSWERING*** ➧ **ADD** unter *Number* ein.

Mit dem CAPI User Concept (siehe Kapitel 7.1.2, Seite 192) können Sie den Zugriff auf die CAPI-Dienste bestimmten Nutzern mit eigenen Paßwörtern vorbehalten.

6.1.5 BinGO! als DHCP-Server einrichten

IP-Adressen im LAN

Jeder Rechner in Ihrem ➤➤ **LAN** benötigt, wie auch **BinGO!**, eine eigene IP-Adresse. Wenn Sie **BinGO!** als ➤➤ **DHCP** (Dynamic Host Configuration Protocol)-Server einrichten, vergibt er anfragenden Rechnern im LAN automatisch ➤➤ **IP-Adressen** aus einem definierten IP-Adreß-Pool. Ein Rechner sendet einen Adreß-Request aus und erhält daraufhin seine IP-Adresse vom **BinGO!** zugewiesen. Sie müssen den Rechnern keine festen IP-Adressen zuweisen, der Konfigurationsaufwand für Ihr Netzwerk verringert sich. Dazu richten Sie einen Pool an IP-Adressen ein, aus dem **BinGO!** jeweils für einen definierten Zeitraum IP-Adressen an Hosts im LAN vergibt. Ein DHCP-Server übermittelt auch die Adressen des statisch oder per PPP-Aushandlung eingetragenen Domain Name Servers (➤➤ **DNS**), ➤➤ **NetBIOS** Name Servers (WINS) und des Standard-➤➤ **Gateway**s.

➤ Gehen Sie zu ***IP*** ➧ ***DHCP SERVER*** ➧ **ADD:**

```
BinGO! Setup Tool                                BinTec Communications AG
[IP][DHCP][ADD]: Add range of IP Addresses                       MyBinGO!


    Interface                                    en1
    IP Address                                   192.168.1.1
    Number of consecutive addresses              8
    Lease Time (Minutes)                         120
    MAC Address


        SAVE                                CANCEL

Use <Space> to select
```

Das Menü enthält folgende Felder:

Feld	Bedeutung
Interface	Schnittstelle, der der folgende Adreß-Pool zugewiesen wird. Wenn ein Adreß-Request über *Interface* eingeht, wird eine der Adressen aus dem Adreß-Pool zugeteilt.
IP Address	Erste IP-Adresse des Adreß-Pools.
Number of consecutive addresses	Anzahl der IP-Adressen im Adreß-Pool, einschließlich der ersten IP-Adresse (*IP Address*).
Lease Time (Minutes)	Legt fest, wie lange eine Adresse aus dem Pool einem Host zugewiesen wird. Nachdem *Lease Time (Minutes)* abgelaufen ist, kann die Adresse anderweitig vergeben werden.
MAC Address	(optional) Nur bei *Number of consecutive addresses = 1:* Nur dem Gerät mit *MAC Address* wird *IP Address* zugewiesen.

Tabelle 6-8: ***IP*** ➧ ***DHCP SERVER*** ➧ **ADD**

ToDo Machen Sie folgende Eintragungen, um **BinGO!** als DHCP-Server einzurichten:

➤ Wählen Sie *Interface* aus, z. B. ***en1***.

- Geben Sie *IP Address* ein, z. B. ***192.168.1.1***.
- Geben Sie *Number of consecutive addresses* ein, z. B. ***8***.
- Geben Sie *Lease Time (Minutes)* ein, z. B. ***120***.
- Geben Sie gegebenenfalls *MAC Address* ein.
- Bestätigen Sie mit **SAVE**.

  Sie befinden sich im Menü ***IP*** ➧ ***DHCP SERVER***, wo die IP-Adreß-Pools aufgelistet sind. Die Eintragungen sind gespeichert.

Sie können auch mehrere Einträge erzeugen und so einen IP-Adreß-Pool aus nicht-zusammenhängenden Adressbereichen definieren, z. B. 192.168.1.20 - 192.168.1.29 und 192.168.1.35 - 192.168.1.40 usw.

6.1.6 Filter setzen

NetBIOS-Filter

Wenn Sie in Ihrem lokalen Netzwerk mit Windows arbeiten, sollten Sie ➤➤ **NetBIOS**-Filter setzen, um Gebühren zu sparen. Dies verhindert, daß **BinGO!** Verbindungen z. B. zum Internet Service Provider (➤➤ **ISP**) aufbaut, um WINS-Requests von Rechnern in Ihrem Netzwerk weiterzugeben. D. h. **BinGO!** fragt beim ISP nach, welcher ➤➤ **Hostname** einer IP-Adresse zugeordnet werden kann. Da der ISP WINS-Namen nicht auflösen kann, sind diese Verbindungen unnötig, kosten aber Gebühren.

Ausführliche Erläuterungen zum Thema ➤➤ **Filter** finden Sie in Kapitel 8.2.8, Seite 258.

Gehen Sie folgendermaßen vor, um diese unnötigen Verbindungen zu verhindern:

Achten Sie darauf, daß Sie sich beim Konfigurieren der Filter nicht selbst aussperren.

- Greifen Sie zur Filter-Konfiguration über die serielle Schnittstelle oder isdn-Login auf **BinGO!** zu.
- Wenn Sie trotzdem über telnet auf **BinGO!** zugreifen, wählen Sie im Menü ***IP*** ➧ ***ACCESS LISTS*** ➧ ***INTERFACES*** ➧ ***EDIT*** *First Rule* aus: *none*.

➤ Gehen Sie zu ***IP*** ➧ ***ACCESS LISTS*** ➧ ***FILTER*** ➧ **ADD**:

```
BinGO! Setup Tool                              BinTec Communications AG
[IP][ACCESS][FILTER][ADD]: Configure IP Access Filter          MyBinGO!

    Description              wrong_dns
    Index                    1

    Protocol                 udp

    Source Address
    Source Mask
    Source Port              specify
    Specify Port             137

    Destination Address
    Destination Mask
    Destination Port         specify
    Specify Port             53

                     SAVE                        CANCEL

Enter string, max length = 48 chars
```

ToDo Machen Sie folgende Eintragungen, um ein Filter zu definieren:

- ➤ Geben Sie *Description* ein: *wrong_dns*.
- ➤ Wählen Sie *Protocol* aus: *udp*.
- ➤ Wählen Sie *Source Port* aus: *specify*.
- ➤ Geben Sie *Specify Port* ein: *137*.
- ➤ Wählen Sie *Destination Port* aus: *specify*.
- ➤ Geben Sie *Specify Port* ein: *53*.
- ➤ Bestätigen Sie mit **SAVE**.

  Sie befinden sich im Menü ***IP*** ➧ ***ACCESS LISTS*** ➧ ***FILTER***. Die Eintragungen sind gespeichert.

Definieren Sie nun ein zweites Filter wie folgt:

- ➤ Gehen Sie erneut zu ***IP*** ➧ ***ACCESS LISTS*** ➧ ***FILTER*** ➧ **ADD**.
- ➤ Geben Sie *Description* ein: *all*.
- ➤ Wählen Sie *Protocol* aus: *any*.
- ➤ Wählen Sie *Source Port* aus: *any*.

- Wählen Sie *Destination Port* aus: *any*.
- Bestätigen Sie mit **SAVE**.

  Sie befinden sich wieder im Menü ***IP*** ➧ ***ACCESS LISTS*** ➧ ***FILTER***. Die Eintragungen sind gespeichert, beide Filter sind aufgelistet.

Gehen Sie folgendermaßen vor, um für diese Filter Regeln festzulegen:

- Gehen Sie zu ***IP*** ➧ ***ACCESS LISTS*** ➧ ***RULES*** ➧ **ADD**:

```
BinGO! Setup Tool                              BinTec Communications AG
[IP][ACCESS][RULE][ADD]: Configure IP Access Rules            MyBinGO!


    Action               deny M
    Filter               wrong_dns (1)


                 SAVE                      CANCEL

Use <Space> to select
```

ToDo Machen Sie folgende Eintragungen, um eine Regel zu definieren:

- Wählen Sie *Action* aus: *deny M*.
- Wählen Sie *Filter* aus: *wrong_dns (1)*.
- Bestätigen Sie mit **SAVE**.

  Sie befinden sich im Menü ***IP*** ➧ ***ACCESS LISTS*** ➧ ***RULES***. Die Eintragungen sind gespeichert.

Definieren Sie nun eine zweite Regel wie folgt:

- Gehen Sie erneut zu ***IP*** ➧ ***ACCESS LISTS*** ➧ ***RULES*** ➧ **ADD**.
- Wählen Sie *Insert behind Rule* aus: *RI 1 FI 1 (wrong_dns)*.
- Wählen Sie *Action* aus: *allow M*.
- Wählen Sie *Filter: all (2)*.
- Bestätigen Sie mit **SAVE**.

  Sie befinden sich wieder im Menü ***IP*** ➧ ***ACCESS LISTS*** ➧ ***RULES***. Die Eintragungen sind gespeichert und aufgelistet:

```
BinGO! Setup Tool                              BinTec Communications AG
[IP][ACCESS][RULE]: Configure IP Access Rules                  MyBinGO!

Abbreviations:   RI (Rule Index)  M  (Action if filter matches)
                 FI (Filter Index)!M (Action if filter does not match)
                 NRI (Next Rule Index)

RI  FI  NRI      Action  Filter      Conditions
1   1   2        deny  M wrong_dns   udp, sp 137, dp 53
2   2   0        allow M all

        ADD              DELETE           REORG            EXIT

Press <Ctrl-n>,<Ctrl-p> to scroll,<Space> tag/untag DELETE,<Return> to
edit
```

➤ Gehen Sie zu ***IP*** ➧ ***ACCESS LISTS*** ➧ ***INTERFACES***:

```
BinGO! Setup Tool                              BinTec Communications AG
[IP][ACCESS][INTERFACES]: Configure First Rule                 MyBinGO!

    Configure first rules for interfaces

    Interface    First Rule       First Filter
    en1          1                1  (wrong_dns)
    en1-snap     1                1  (wrong_dns)


    EXIT

Press <Ctrl-n>, <Ctrl-p> to scroll, <Return> to edit/select
```

ToDo Machen Sie folgende Eintragungen:

➤ Wählen Sie die LAN-Schnittstelle von **BinGO!** (*en1* bzw. *en1-snap*) und bestätigen Sie mit der **Eingabetaste**.

➤ Wählen Sie *First Rule* aus: *RI 1 FI 1 (wrong_dns)*.

➤ Bestätigen Sie mit **SAVE**.

Mit diesen Eintragungen haben Sie erreicht, daß aller Datenverkehr, der vom Quell-➤➤ **Port** 137 zum Ziel-Port 53 verläuft, verworfen wird. Somit werden keine unnötigen Verbindungen aufgebaut, um WINS-Namen aufzulösen.

➤ Verlassen Sie ***IP*** ➧ ***ACCESS LISTS*** ➧ ***INTERFACES*** mit **EXIT**.

- Verlassen Sie ***IP*** ➧ ***ACCESS LISTS*** mit **EXIT**.
- Verlassen Sie ***IP*** mit **EXIT**.

  Sie befinden sich wieder im Hauptmenü.

  Die Konfiguration der grundlegenden Routereinstellungen ist abgeschlossen.
- Verlassen Sie das Hauptmenü mit **Exit** und speichern Sie die erstellte Konfiguration mit **Save as boot configuration and exit**.

  Die Einstellungen sind damit im Flash gespeichert und gehen beim Ausschalten von **BinGO!** nicht verloren (siehe Kapitel 6.3, Seite 187).

6.2 BinGO! und das WAN

Wenn Sie die Konfigurationsschritte in Kapitel 6.1, Seite 125 durchgeführt haben, ist **BinGO!** für Ihr ➤➤ **LAN** eingerichtet. Wenn Sie auch auf Hosts außerhalb Ihres LANs zugreifen wollen, z. B. um im ➤➤ **Internet** zu surfen, ist dieses Kapitel interessant für Sie.

Folgende Punkte werden behandelt:

- Einrichten eines ➤➤ **WAN-Partner**s allgemein:
  Um mit **BinGO!** Verbindungen zu Netzwerken außerhalb Ihres LANs herstellen zu können, müssen Sie die gewünschten Verbindungspartner als WAN-Partner auf **BinGO!** einrichten. Dies gilt sowohl für ausgehende Verbindungen (**BinGO!** wählt sich bei einem WAN-Partner ein), als auch für eingehende Verbindungen (ein WAN-Partner wählt sich bei **BinGO!** ein). Wenn Sie einen Internetzugang herstellen wollen, müssen Sie Ihren Internet Service Provider (➤➤ **ISP**) als WAN-Partner einrichten. Wenn Sie eine LAN-LAN-Kopplung aufbauen wollen, z. B. zwischen Ihrem LAN und dem LAN Ihrer Firmenzentrale (Firmennetzanbindung), müssen Sie das LAN der Firmenzentrale als WAN-Partner einrichten.
  In folgenden Kapitel 6.2.1, Seite 152, wird in allgemeiner Form erläutert, wie Sie vorgehen, um einen WAN-Partner auf **BinGO!** einzurichten.

- Einrichten eines WAN-Partners für Zugang zum Internet (anhand von Beispielen):
  In Kapitel 6.2.2, Seite 176 finden Sie Beispiele für das Einrichten eines Internet Service Providers als WAN-Partner. Wenn Sie Ihren Internetzugang über einen der folgenden Provider ausführen, finden Sie dort eine schnelle Vorgehensweise, um mit **BinGO!** ins Internet zu gelangen:
  – T-Online
  – Compuserve

- Einrichten eines WAN-Partners zur Firmennetzanbindung anhand eines Beispiels:
  In Kapitel 6.2.3, Seite 183 finden Sie ein Beispiel für das Einrichten einer Firmennetzanbindung auf **BinGO!**. In den meisten Fällen sollte diese schnelle Vorgehensweise ausreichend sein.

In Bild 6-3, Seite 151 ist ein grundlegendes Szenario abgebildet, wie eine Verbindung zu den WAN-Partnern Internet Service Provider und Firmenzentrale aussehen könnte!

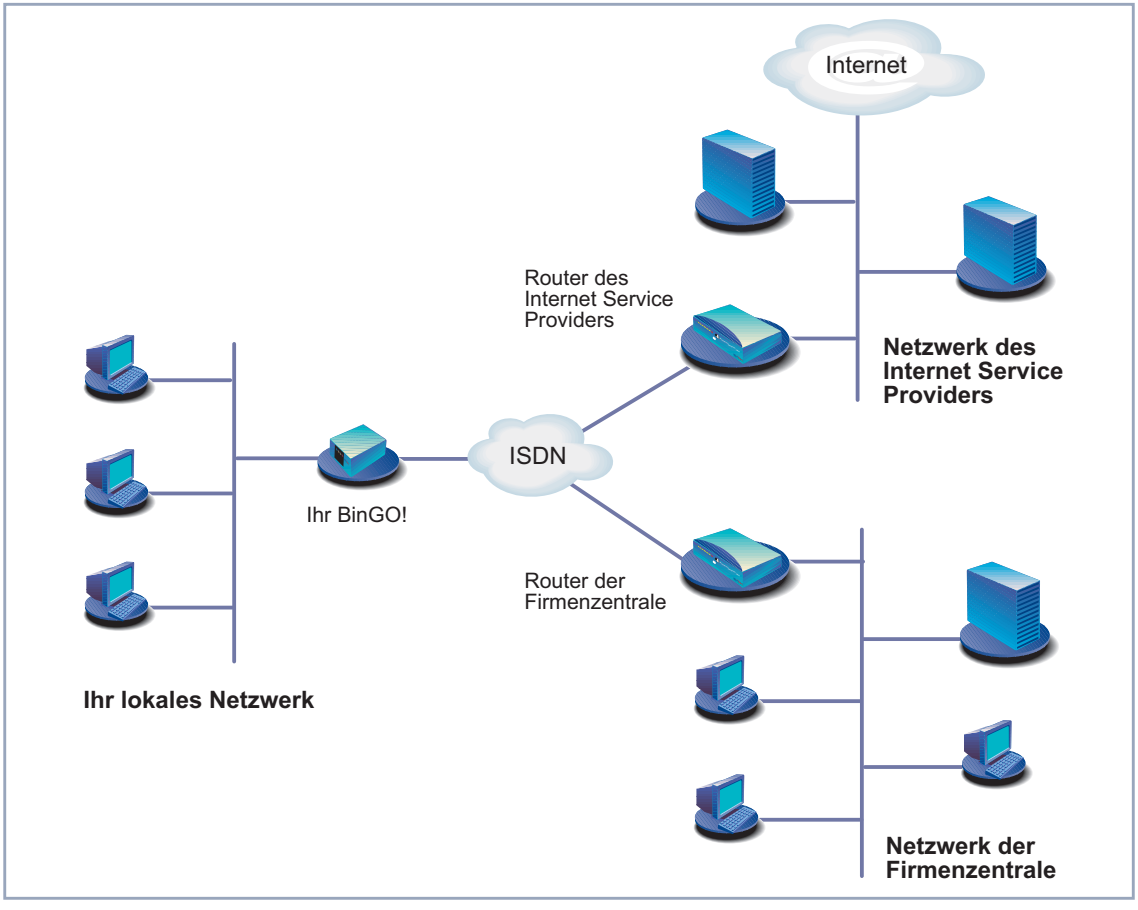


Bild 6-3: Grundszenario

6.2.1 WAN-Partner einrichten

Das Einrichten eines WAN-Partners umfaßt im allgemeinen die folgenden Schritte:

- WAN-Partner eintragen:
  - ➤➤ **Protokoll** festlegen.
  - Rufnummer(n) eintragen.
  - ➤➤ **PPP**-Einstellungen zur Authentisierung festlegen.
  - ➤➤ **Shorthold** festlegen.
  - IP-Konfiguration durchführen.
- Routing-Eintrag erstellen
- Network Address Translation (➤➤ **NAT**) aktivieren (optional)

Los geht's:

WAN-Partner eintragen

WAN-Partner einrichten

Damit richten Sie einen Zugang zu dem gewünschten WAN-Partner, z. B. Ihrem Internet Service Provider (ISP), ein. Bevor Sie zur Tat schreiten, sollten Sie sich die dafür notwendigen Zugangsdaten, die Sie von Ihrem ISP oder System-Administrator erhalten haben, zurechtlegen (siehe Kapitel 3.2.1, Seite 40). Die Bezeichnungen können unter Umständen von Provider zu Provider leicht variieren.

Gehen Sie folgendermaßen vor, um einen WAN-Partner einzutragen:

➤ Gehen Sie zu ***WAN PARTNER:***

```
BinGO! Setup Tool                                BinTec Communications AG
[WAN]: WAN Partners                                              MyBinGO!

Current WAN Partner Configuration

    Partnername              Protocol        State
    BigBoss                  ppp             dormant



ADD                 DELETE               EXIT


Press <Ctrl-n>,<Ctrl-p> to scroll,<Space> tag/untag DELETE,<Return> to
edit
```

Hier sind die aktuell eingetragenen WAN-Partner mit *Partnername*, *Protocol* und *State* aufgelistet. *State* kann folgende Werte annehmen:

- *up:* verbunden
- *dormant:* nicht verbunden
- *blocked:* nicht verbunden (aufgrund eines Fehlers beim Verbindungsaufbau ist ein erneuter Versuch erst nach einer definierten Anzahl von Sekunden möglich, siehe Kapitel 7.2.1, Seite 201)
- *down:* administrativ auf down gesetzt

Gehen Sie folgendermaßen vor, um einen Eintrag in der Liste vorzunehmen:

➤ Fügen Sie mit **ADD** einen neuen Eintrag hinzu oder wählen Sie einen bestehenden Eintrag aus. Bestätigen Sie mit der **Eingabetaste**, um den Eintrag zu ändern.

Ein weiteres Menüfenster erscheint:

```
BinGO! Setup Tool                              BinTec Communications AG
[WAN][ADD]:Configure WAN Partner                                MyBinGO!

    Partner Name                 BigBoss

    Encapsulation                PPP
    Compression                  none
    Encryption                   none
    Calling Line Identification  no

    WAN Numbers >
    PPP >
    Advanced Settings >

    IP >
    IPX >

                     SAVE                      CANCEL

Enter string, max length = 25 chars
```

Das Menü enthält folgende Felder:

Feld	Bedeutung
Partner Name	Geben Sie einen beliebigen Namen ein, um den WAN-Partner eindeutig zu benennen.

Feld	Bedeutung
Encapsulation	➤➤ **Enkapsulierung**. Definiert, wie die ➤➤ **Daten-Pakete** für die Übertragung zum WAN-Partner enkapsuliert werden. Mögliche Werte: ■ *PPP* ■ *Multi-Protocol LAPB Framing* ■ *Multi-Protocol HDLC Framing* ■ *Async PPP over X.75* ■ *Async PPP over X.75/T.70/BTX* ■ *X.25_PPP:* auf **BinGO!** nicht verfügbar ■ *X.25:* auf **BinGO!** nicht verfügbar ■ *HDLC Framing (only IP)* ■ *LAPB Framing (only IP)* ■ *X31 B-Channel:* auf **BinGO!** nicht verfügbar ■ *X.25 No Signalling:* auf **BinGO!** nicht verfügbar ■ *X.25 PAD:* auf **BinGO!** nicht verfügbar ■ *X.25 No Configuration:* auf **BinGO!** nicht verfügbar ■ *Frame Relay:* auf **BinGO!** nicht verfügbar ■ *X.25 No Configuration, No Signalling:* auf **BinGO!** nicht verfügbar

Feld	Bedeutung
Compression	Legt die Art der Komprimierung fest, die für den Datenverkehr mit dem WAN-Partner angewendet werden soll. Mögliche Werte: ■ *STAC:* nur bei *Encapsulation* = *PPP* ■ *MS-STAC:* nur bei *Encapsulation* = *PPP* ■ *MPPC:* auf **BinGO!** nicht verfügbar ■ *V.42bis:* nur bei *Encapsulation* = *Multi-Protocol LAPB Framing* oder *LAPB Framing (only IP)* ■ *none*
Encryption	Definiert die Art der Verschlüsselung, die für den Datenverkehr mit dem WAN-Partner angewendet werden soll. Nur möglich, wenn keine Komprimierung mit STAC auf der Verbindung aktiviert ist. Mögliche Werte: ■ *MPPE 40:* nur bei *Encapsulation* = *PPP* ■ *MPPE 128:* nur bei *Encapsulation* = *PPP* und *Authentication* = *MS-CHAP* ■ *none*
Calling Line Identification	Zeigt an, ob Rufe von diesem WAN-Partner anhand der Calling Party's Number identifiziert werden sollen (➤➤ **CLID**). Der Wert des Feldes ist abhängig von *Direction* im Untermenü ***WAN NUMBERS*** und kann hier nicht gesetzt werden.

Tabelle 6-9: ***WAN PARTNER*** ➧ **ADD**

In der folgenden Tabelle ist dargestellt, welche Enkapsulierungen welche Verfahren zur ➤➤ **Datenkomprimierung** unterstützen:

Protokolle		Enkapsulierung	Komprimierung	
IP	IPX		STAC, MS-STAC	V.42bis
X	X	*PPP*	X	
X	X	*Async PPP over X.75*	X	
X	X	*Async PPP over X.75/T.70/BTX*	X	
X	X	*Multi-Protocol LAPB Framing*		X
X	X	*Multi-Protocol HDLC Framing*		
X		*HDLC Framing (only IP)*		
X		*LAPB Framing (only IP)*		X

Tabelle 6-10: Enkapsulierung und Komprimierung

ToDo Machen Sie folgende Eintragungen:

- Geben Sie *Partner Name* ein, z. B. ***BigBoss***.
- Wählen Sie *Encapsulation* aus, z. B. ***PPP***.
- Wählen Sie *Compression* aus, z. B. ***none***.
- Wählen Sie *Encryption* aus, z. B. ***none***.
- Gehen Sie zu ***WAN PARTNER*** ➧ **ADD** ➧ ***WAN NUMBERS***:

Rufnummern eintragen

```
BinGO! Setup Tool                              BinTec Communications AG
[WAN][ADD][WAN Numbers]: WAN Numbers (BigBoss)                MyBinGO!


    WAN Numbers for this partner:

        WAN Number           Direction
        0911987654321        outgoing



    ADD                  DELETE                    EXIT

Press <Ctrl-n>,<Ctrl-p> to scroll,<Space> tag/untag DELETE,<Return> to
edit
```

Hier sind die aktuell eingetragenen Rufnummern des WAN-Partners aufgelistet.

Gehen Sie folgendermaßen vor, um einen Eintrag in der Liste vorzunehmen:

- Fügen Sie mit **ADD** einen neuen Eintrag hinzu oder wählen Sie einen bestehenden Eintrag aus. Bestätigen Sie mit der **Eingabetaste**, um den Eintrag zu ändern.

  Ein weiteres Menüfenster erscheint:

```
BinGO! Setup Tool                              BinTec Communications AG
[WAN][ADD][WAN NUMBERS][ADD]:Add or Change WAN Numbers(BigBoss)
                                                                MyBinGO!


    Number                  0911987654321
    Direction               outgoing

    Advanced Settings >


            SAVE                          Cancel

Enter string, max length = 40 chars
```

Das Menü enthält folgende Felder:

Feld	Bedeutung
Number	Rufnummer des WAN-Partners.
Direction	Definiert, ob *Number* für eingehende oder für ausgehende Rufe oder für beides verwendet werden soll.

Tabelle 6-11: ***WAN PARTNER*** ➧ **ADD** ➧ ***WAN NUMBERS*** ➧ **ADD**

Das Feld *Direction* enthält folgende Auswahlmöglichkeiten:

Mögliche Werte	Bedeutung
outgoing	Für ausgehende Rufe, wenn Sie sich beim WAN-Partner einwählen wollen.
both (CLID)	Für eingehende und ausgehende Rufe.
incoming (CLID)	Für eingehende Rufe, wenn der WAN-Partner sich bei **BinGO!** einwählen soll.

Tabelle 6-12: *Direction*

Wenn **BinGO!** 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 Sie können einzelne Ziffern oder Gruppen von Ziffern durch Wildcards ersetzen. Damit kann *Number* mit verschiedenen Rufnummern übereinstimmen.

Folgende Wildcards können Sie benutzen, was sich bei eingehenden und ausgehenden Rufen unterschiedlich auswirkt:

Wildcard	Bedeutung		Beispiel		
	Eingehende Rufe	Ausgehende Rufe	Number	**BinGO!** akzeptiert eingehende Rufe z. B. mit:	Ausgehende Rufe, d. h. **BinGO!** 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

Wildcard	Bedeutung		Beispiel		
	Eingehende Rufe	Ausgehende Rufe	Number	BinGO! akzeptiert eingehende Rufe z. B. mit:	Ausgehende Rufe, d. h. BinGO! baut eine Verbindung zum WAN-Partner auf mit:
{ab}	Entspricht einer Gruppe von optionalen Ziffern.	Wird verwendet.	{00}1234	00123 und 123	00123

Tabelle 6-13: Wildcards für ein- und ausgehende Rufe

Wenn die Calling Party's 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.

ToDo Machen Sie die folgenden Eintragungen:

- Geben Sie *Number* ein, z. B. ***0911987654321***.
- Wählen Sie *Direction* aus, z. B. ***outgoing***.
- Bestätigen Sie mit **SAVE**.
  Die Eintragungen sind gespeichert und aufgelistet.
- Verlassen Sie ***WAN PARTNER*** ➧ **ADD** ➧ ***WAN NUMBERS*** mit **EXIT**.

➤➤ PPP-Authentisierung

Tragen Sie als nächstes die ➤➤ **PPP**-Einstellungen des WAN-Partners ein. Sie dienen zur Authentisierung der Verbindungspartner.

Wenn ein Ruf eingeht, wird über den ISDN-➤➤ **D-Kanal** die Nummer des Anrufers mitgegeben. Anhand dieser Nummer kann **BinGO!** den Anrufer identifizieren (➤➤ **CLID**), wenn dieser als WAN-Partner eingetragen ist. Nach der Identifizierung mit CLID kann der Router zusätzlich eine PPP-Authentisierung mit dem WAN-Partner durchführen, bevor der Ruf angenommen wird. Dazu benötigt der Router Vergleichsdaten, die Sie hier eintragen. Zunächst legen Sie fest, welche Authentisierungsverhandlung ausgeführt werden soll, anschlie-

ßend tragen Sie ein gemeinsames Paßwort und zwei Kennungen ein. Diese Daten erhalten Sie z. B. von Ihrem Internet Service Provider oder dem System-Administrator der Firmenzentrale. Nur wenn diese Daten, die Sie auf **BinGO!** hier eintragen, mit den Daten des Anrufers übereinstimmen, wird der Ruf angenommen.

Gehen Sie folgendermaßen vor, um die PPP-Authentisierung des WAN-Partners festzulegen:

➤ Gehen Sie zu ***WAN PARTNER*** ➧ **ADD** ➧ ***PPP***:

```
BinGO! Setup Tool                              BinTec Communications AG
[WAN][ADD][PPP]: PPP Settings (BigBoss)                        MyBinGO!


    Authentication              CHAP + PAP
    Partner PPP ID              BigBoss
    Local PPP ID                LittleIndian
    PPP Password                Secret

    Keepalives                  off
    Link Quality Monitoring     off


                OK                              CANCEL

Use <Space> to select
```

Das Menü enthält folgende Felder:

Feld	Bedeutung
Authentication	Authentisierungsprotokoll.
Partner PPP ID	Kennung des WAN-Partners.
Local PPP ID	**BinGO!**s Kennung.
PPP Password	Paßwort.
Keepalives	Aktiviert Keepalive-Pakete.
Link Quality Monitoring	PPP Link Quality Monitoring nach RFC 1989.

Tabelle 6-14: ***WAN PARTNER*** ➧ **ADD** ➧ ***PPP***

Das Feld *Authentication* enthält folgende Auswahlmöglichkeiten:

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

Tabelle 6-15: *Authentication*

ToDo Machen Sie folgende Eintragungen:

- Wählen Sie *Authentication* aus, z. B. ***CHAP***.
- Geben Sie *Partner PPP ID* ein, z. B. ***BigBoss***.
- Geben Sie *Local PPP ID* ein, z. B. ***LittleIndian***.
- Geben Sie *PPP Password* ein, z. B. ***Secret***.
- Wählen Sie *Keepalives* aus, z. B. ***off***.
- Wählen Sie *Link Quality Monitoring* aus, z. B. ***off***.
- Bestätigen Sie mit **OK**.
  Sie befinden sich im Menü ***WAN PARTNER*** ➧ **ADD**.

In manchen Fällen kann der Anrufer nicht per ➤➤ **CLID** identifiziert werden, obwohl er als WAN-Partner eingetragen ist. In diesem Fall weiß **BinGO!** nicht, welches Authentisierungsprotokoll mit diesem WAN-Partner festgelegt ist. Damit der Ruf trotzdem angenommen werden kann, greift **BinGO!** auf allgemeine Einstellungen im PPP zurück, die Sie nach Bedarf verändern können (siehe Kapitel 7.1.4, Seite 198).

Shorthold festlegen

Stellen Sie als nächstes Shorthold ein, um Gebühren zu sparen. **BinGO!** bricht dann die ISDN-Verbindung ab, wenn keine Daten mehr fließen. Mit statischem bzw. dynamischem Shorthold legen Sie fest, nach welchem Inaktivitätsintervall (Idle Timer) **BinGO!** die ISDN-Verbindung abbauen soll.

Statisch

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

Dynamisch

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

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

Bitte beachten Sie: dynamischen Shorthold können Sie nur nutzen, wenn Sie die Gebühreninfomrationen während der Verbindung empfangen. Fragen Sie Ihre Telefongesellschaft!

Es ist unbedingt notwendig, bei Nutzung des dynamischen Shortholds zusätzlich einen statischen Shorthold einzustellen, um beim Ausfall von AOCD keine Dauer➤➤ **wählverbindung** zu haben.

Dabei sollten Sie darauf achten, daß der statische Shorthold später einsetzt als der dynamische. Andernfalls beendet **BinGO!** die Verbindung immer gemäß dem statischen Shorthold, der dynamische Shorthold kann nicht greifen. Geben Sie deshalb in diesem Fall als *Static Short Hold (sec)* einen Wert ein, der etwas über dem maximal zu erwartenden dynamischen Inaktivitätsintervall liegt.

In Deutschland unterstützen andere Anbieter als die Telekom derzeit keine Gebühreninformationen.

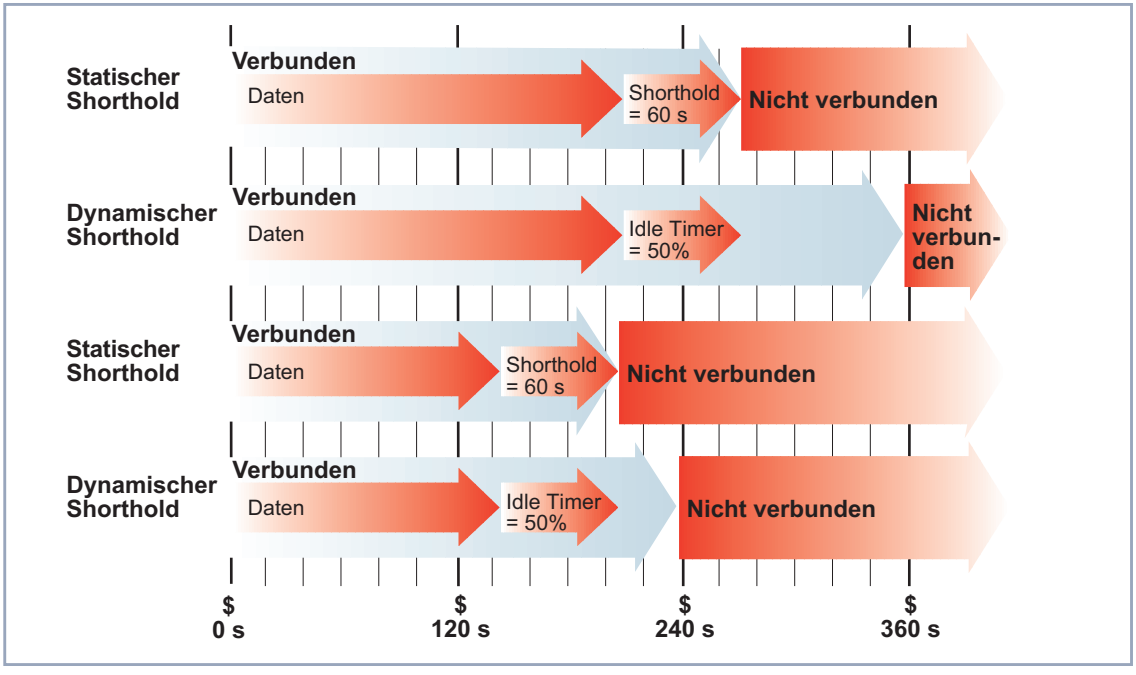


Bild 6-4: Dynamischer und statischer Shorthold

Gehen Sie folgendermaßen vor:

➤ Gehen Sie zu ***WAN PARTNER*** ➧ **ADD** ➧ ***ADVANCED SETTINGS***:

```
BinGO! Setup Tool                              BinTec Communications AG
[WAN][ADD][ADVANCED]: Advanced Settings (BigBoss)             MyBinGO!


Callback                                 no
Static Short Hold (sec)                  20
Idle for Dynamic Short Hold (%)          0
Delay after Connection Failure (sec)     300

Channel-Bundling                         no

Layer 1 Protocol                         ISDN 64 kbps


                OK                                    CANCEL

Use <Space> to select
```

Folgende Teile des Menüs sind für diesen Konfigurationsschritt relevant:

Feld	Bedeutung
Static Short Hold (sec)	Inaktivitätsintervall in Sekunden für statischen Shorthold. Beispielwerte für Fernverbindungen: *60*, wenn Gebühreninformationen während der Verbindung übermittelt werden (AOCD). *20* sonst.
Idle for Dynamic Short Hold (%)	Inaktivitätsintervall in % für dynamischen Short-hold. Nur wirksam, wenn Gebühreninformationen während der Verbindung übermittelt werden (AOCD).

Tabelle 6-16: ***WAN PARTNER*** ➧ **ADD** ➧ ***ADVANCED SETTINGS***

ToDo Machen Sie folgende Eintragungen:

- Geben Sie *Static Short Hold (sec)* ein, z. B. ***20***.
- Geben Sie *Idle for Dynamic Short Hold (%)* ein, z. B. ***0***.
- Bestätigen Sie mit **OK**.
  Sie befinden sich im Menü ***WAN PARTNER*** ➧ **ADD**.

Tips für die Eingabe von *Idle for Dynamic Short Hold (%):*

- Für interaktive Verbindungen (z. B. ➤➤ **telnet**) sollten Sie einen hohen Wert eingeben (z. B. 80...90), um Verbindungsabbrüche während kurzer Phasen ohne Datenfluß zu vermeiden.
- Für Internet-Verbindungen (z. B. WWW, http, usw.) sollten Sie einen mittleren bis hohen Wert eingeben (z. B. 50...80), um Verbindungsabbrüche während Wartephasen zu vermeiden.
- Für Daten-Verbindungen (z. B. ➤➤ **ftp**) sollten Sie einen niedrigen Wert eingeben (z. B. 10...40), um ein unnötiges Offenhalten von Verbindungen zu vermeiden, nachdem der Datentransfer abgeschlossen ist.

Nähere Erläuterungen zum statischen und dynamischen Shorthold finden Sie in der Software Reference.

IP-Konfiguration durchführen

Nehmen Sie als nächstes die IP-Konfiguration des WAN-Partners vor. Hier tragen Sie die ➤➤ **IP-Adresse** und ➤➤ **Netzmaske** des Partners ein.

Gehen Sie folgendermaßen vor:

➤ Gehen Sie zu ***WAN PARTNER*** ➧ **ADD** ➧ ***IP***:

```
BinGO! Setup Tool                                BinTec Communications AG
[WAN][ADD][IP]: IP Configuration (BigBoss)                      MyBinGO!


    IP Transit Network                    no


    Partner's LAN IP Address              10.1.1.0
    Partner's LAN Netmask                 255.255.255.0

    Advanced Settings >

                    SAVE                      CANCEL

Use <Space> to select
```

Das Menü enthält folgende Felder:

Feld	Bedeutung
IP Transit Network	Legt fest, ob **BinGO!** ein Transit Network zum WAN-Partner aufbaut.
local ISDN IP Address	ISDN-IP-Adresse von **BinGO!** im Transit Network.
Partner's ISDN IP Address	ISDN-IP-Adresse des WAN-Partners im Transit Network.
Partner's LAN IP Address	IP-Adresse des LAN des WAN-Partners.
Partner's LAN Netmask	Netzmaske des LAN des WAN-Partners. Wenn Sie keinen Eintrag machen, trägt **BinGO!** eine Standard-Netzmaske für die unter *Partner's LAN IP Address* verwendete Netzklasse ein.

Tabelle 6-17: ***WAN PARTNER*** ➧ **ADD** ➧ ***IP***

ToDo Machen Sie folgende Eintragungen (bei einer Firmennetzanbindung normalerweise ausreichend):

- Wählen Sie *IP Transit Network* aus: z. B. ***no***.
- Geben Sie *Partner's LAN IP Address* ein, z. B. ***10.1.1.0***.
- Geben Sie *Partner's LAN Netmask* ein, z. B. ***255.255.255.0***.

- Bestätigen Sie mit **SAVE**.
- Bestätigen Sie nochmals mit **SAVE**.

  Sie befinden sich wieder in ***WAN PARTNER***. Ihre Eintragungen sind gespeichert.

Wenn Sie einen Internetzugang einrichten, kennen Sie normalerweise die IP-Adresse Ihres Internet Service Providers (ISP) nicht und **BinGO!** bekommt die *local ISDN IP Address* dynamisch (für die Dauer der Verbindung) oder statisch vom ISP zugewiesen. Machen Sie in diesem Fall folgende Einstellungen in ***WAN PARTNER*** ➧ **ADD** ➧ ***IP:***

- IP-Adresse wird dynamisch zugewiesen:
  - Wählen Sie *IP Transit Network* aus: *dynamic client*.
- IP-Adresse wird statisch zugewiesen:
  - Wählen Sie *IP Transit Network* aus: yes.
  - *Local ISDN IP Address:* **BinGO!**s statische IP-Adresse, die Sie vom ISP erhalten (oft bezeichnet als Ihr Gateway oder Ihre Router-Adresse).
  - *Partner's ISDN IP Address:* Die IP-Adresse des Partners (falls bekannt), sonst ebenfalls **BinGO!**s statische IP-Adresse, die Sie vom ISP erhalten.
  - Keine Eintragungen für *Partner's LAN IP Address* und *Partner's LAN Netmask*.

Wenn Sie mehr wissen wollen, z. B. was ein Transit Network eigentlich ist und wofür Sie es brauchen, siehe Kapitel 7.2.4, Seite 205.

Um den Domain Name Server des ISP während der Verbindung zu nutzen, machen Sie folgende Einstellungen in ***WAN PARTNER*** ➧ **ADD** ➧ ***IP*** ➧ ***ADVANCED SETTINGS:***

- Wählen Sie *Dynamic Name Server Negotiation* aus: *client (receive)*.

Diese Einstellung ist nur nötig, wenn Sie keine festen IP-Adressen für DNS-Server auf den Rechnern in Ihrem Netz haben.

Routing-Eintrag erstellen

Routing-Eintrag erstellen

Sie haben jetzt einen WAN-Partner auf **BinGO!** eingetragen. Für jeden WAN-Partner wird automatisch ein Routing-Eintrag in der Routing-Tabelle von **BinGO!** erzeugt. Die Routing-Einträge können Sie ändern und weitere hinzufügen. Für die Verbindung zu Ihrem Internet Service Provider sollten Sie immer eine sog. Default-Route einrichten.

Gehen Sie folgendermaßen vor:

➤ Gehen Sie zu ***IP*** ➧ ***ROUTING:***

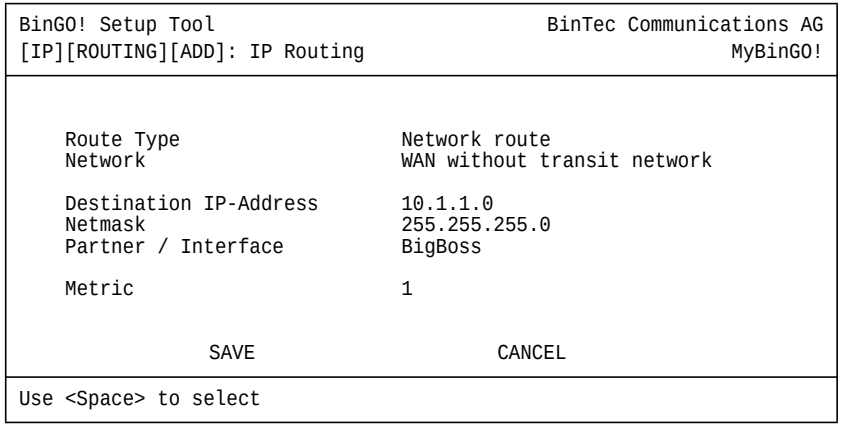
```
BinGO! Setup Tool                              BinTec Communications AG
[IP][ROUTING]: IP Routing                                      MyBinGO!

The flags are:  U (Up), D (Dormant), B (Blocked),
                G (Gateway Route), I (Interface Route)
                S (Subnet Route), H (Host Route)

Destination  Gateway          Mask         Flags    Met  Interface    Pro
192.168.1.1  192.168.1.254    255.255.255.0US       0    en1          loc
10.1.1.0                      255.255.255.0DI       0    BigBoss      mgmt
default                       0.0.0.0      DI       0    GoInternet   mgmt

    ADD             DELETE              EXIT

Press <Ctrl-n>,<Ctrl-p> to scroll,<Space> tag/untag DELETE,<Return> to
edit
```

Hier sind alle eingetragenen IP-Routen aufgelistet. 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) angezeigt. Unter *Pro* wird angezeigt, mit welchem Protokoll **BinGO!** den Routing-Eintrag "gelernt" hat.

Gehen Sie folgendermaßen vor, um eine Route festzulegen:

➤ Fügen Sie mit **ADD** einen neuen Eintrag hinzu oder wählen Sie einen bestehenden Eintrag aus. Bestätigen Sie mit der **Eingabetaste**, um den Eintrag zu ändern.

Ein weiteres Menüfenster erscheint:



Das Menü enthält folgende Felder:

Feld	Bedeutung
Route Type	Art der Route. Mögliche Werte: ■ *Host route:* Route zu einem einzelnen Host ■ *Network route:* Route zu einem Netzwerk ■ *Default route:* Wird nur benutzt, wenn keine andere passende Route verfügbar ist
Network	Definiert die Art der Verbindung (LAN, WAN).
Destination IP-Address	IP-Adresse des Ziel-Hosts oder -LANs.
Netmask	Netzmaske des Partner-LANs (nur möglich bei *Route Type* = *Network route*. Wenn keine Eintragung gemacht wird, benutzt der Router eine Standardnetzmaske).
Partner / Interface	WAN-Partner (nur möglich bei *Network* = *WAN without transit network*)
Gateway IP-Address	IP-Adresse des Hosts, an den **BinGO!** die IP-Pakete weitergeben soll.
Metric	Je niedriger der Wert, desto höhere Priorität besitzt die Route. (Wertebereich 1...14)

Tabelle 6-18: ***IP*** ➧ ***ROUTING*** ➧ **ADD**

Das Feld *Network* enthält folgende Auswahlmöglichkeiten:

Mögliche Werte	Bedeutung
LAN	Route zu einem Ziel-Host oder -LAN, das über **BinGO!**s LAN-Anschluß zu erreichen ist.
WAN without transit network	Route zu einem Ziel-Host oder -LAN, das über einen WAN-Partner ohne Transit Network zu erreichen ist.
WAN with transit network	Route zu einem Ziel-Host oder -LAN, das über einen WAN-Partner mit Transit Network zu erreichen ist.
Refuse	**BinGO!** verwirft Datenpakete, die diese Route benutzen, und übermittelt dem Absender eine Meldung, daß das Ziel des Paketes unerreichbar ist.
Ignore	**BinGO!** verwirft Datenpakete, die diese Route benutzen, ohne eine Statusmeldung zu senden.

Tabelle 6-19: *Network*

Sie können auf **BinGO!** nur eine einzige Default-Route eintragen: Wenn Sie also einen Zugang zum Internet einrichten, dann tragen Sie die Route zu Ihrem Internet Service Provider (ISP) als Default-Route ein.
Wenn Sie eine Firmennetzanbindung machen, dann tragen Sie die Route zur Zentrale nur dann als Default-Route ein, wenn Sie keinen Internetzugang über **BinGO!** einrichten.
Wenn Sie sowohl einen Zugang zum Internet, als auch eine Fimennetzanbindung einrichten, dann tragen Sie zum ISP eine Default-Route und zur Firmenzentrale eine Netzwerk-Route ein.

Default-Route

Gehen Sie folgendermaßen vor, um eine Default-Route einzurichten:

➤ Wählen Sie *Route Type* aus: *Default Route*.

- Wählen Sie *Network* aus: *WAN without transit network*.
- Wählen Sie *Partner / Interface* aus: z. B. ***GoInternet***.
- Geben Sie *Metric* ein, z. B. ***1***.
- Bestätigen Sie mit **SAVE**.

  Sie befinden sich in ***IP*** ➧ ***ROUTING***. Die Eintragungen sind gespeichert, die eingetragene oder geänderte Route ist aufgelistet.

Das Netzwerk der Firmenzentrale kann aus mehreren LANs mit unterschiedlichen Netz-IP-Adressen und Netzmasken bestehen (➤➤ **Subnetze**). Wenn Sie also den Zugang zur Firmenzentrale nicht als Default-Route eintragen (z. B. weil Sie schon Ihren Internetzugang als Default-Route eingerichtet haben), dann müssen Sie für jedes Netz, das Sie in der Firmenzentrale erreichen wollen, einen eigenen Routing-Eintrag vornehmen.

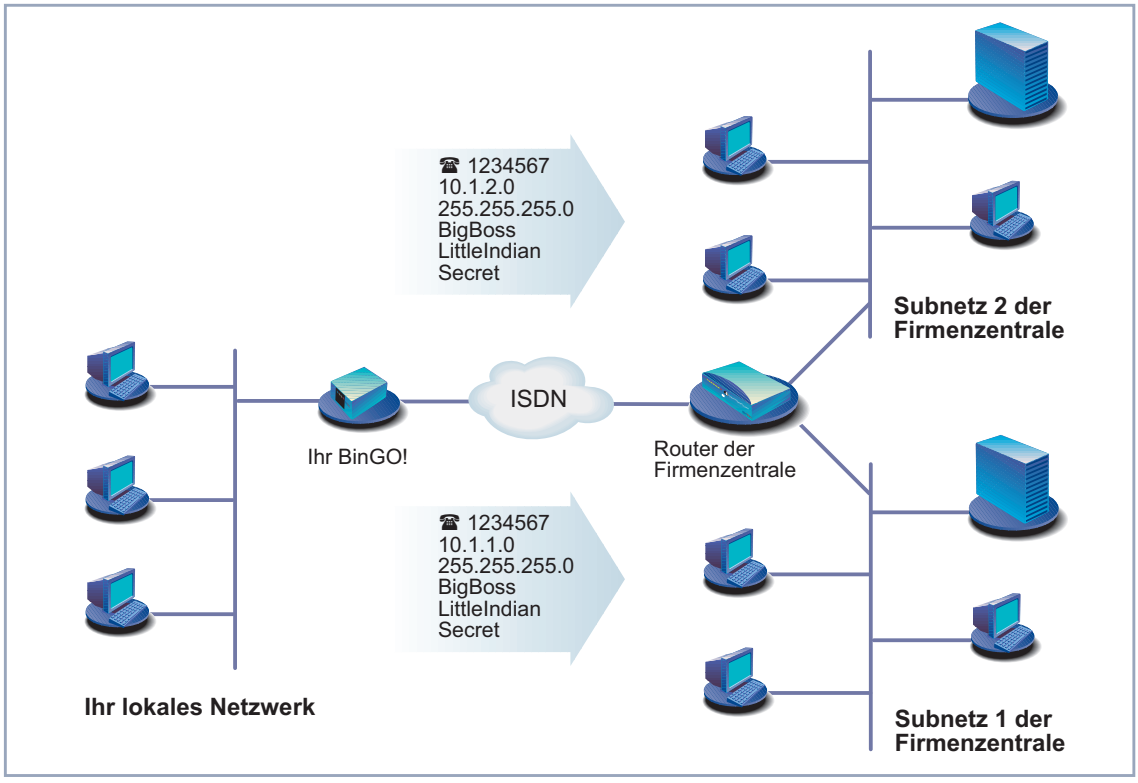


Bild 6-5: Firmennetzzentrale mit mehreren angeschlossenen LANs

Network Route

Gehen Sie folgendermaßen vor, um eine Netzwerk-Route, z. B. für eine Firmennetzanbindung (ohne Default-Route), einzugeben:

- Wählen Sie *Route Type* aus: *Network route*.
- Wählen Sie *Network* aus: *WAN without transit network*.
- Geben Sie *Destination IP-Address* ein, z. B. ***10.1.2.0***.
- Geben Sie *Netmask* ein, z. B. ***255.255.255.0***.
- Geben Sie *Partner / Interface* ein, z. B. ***BigBoss***.
- Geben Sie *Metric* ein, z. B. ***1***.

➤ Bestätigen Sie mit **SAVE**.

Sie befinden sich wieder im Menü ***IP*** ➧ ***ROUTING***. Die Eintragungen sind gespeichert, die eingetragene oder geänderte Route ist aufgelistet.

➤ Wiederholen Sie diese Schritte, wenn Sie mehrere Routen eintragen wollen.

Network Address Translation (NAT) aktivieren

NAT aktivieren

Hier haben Sie die Möglichkeit, für Ihren WAN-Partner Network Address Translation (➤➤ **NAT**) zu aktivieren. Damit verbergen Sie Ihr gesamtes Netzwerk nach außen hinter nur einer IP-Adresse. Für die Verbindung zum Internet Service Provider (ISP) sollten Sie dies auf jeden Fall tun.

Detaillierte Informationen zu Network Address Translation (NAT) finden Sie in Kapitel 8.2.7, Seite 252.

Gehen Sie folgendermaßen vor, um NAT zu aktivieren:

➤ Gehen Sie zu ***IP*** ➧ ***NETWORK ADDRESS TRANSLATION***:

```
BinGO! Setup Tool                              BinTec Communications AG
[IP][NAT]: NAT Configuration                                   MyBinGO!

Select IP Interface to be configured for NAT

GoInternet
BigBoss
en1
en1-snap


EXIT

Press <Ctrl-n>, <Ctrl-p> to scroll, <Return> to edit/select
```

➤ Markieren Sie die Schnittstelle bzw. den WAN-Partner, für den Sie NAT aktivieren wollen (z. B. ***GoInternet***) und bestätigen Sie mit der **Eingabetaste**.

Ein weiteres Menü erscheint:

```
BinGO! Setup Tool                              BinTec Communications AG
[IP][NAT][CONFIG]: NAT Configuration (GoInternet)              MyBinGO!

Network Address Translation      on

Configuration for sessions requested from outside

Service      Destination      Source Dep.      Dest. Dep.   Port Remap


    ADD              DELETE               SAVE             CANCEL

Use <Space> to select
```

ToDo Machen Sie folgende Eintragungen:

- Wählen Sie *Network Address Translation* aus: *on*.
- Bestätigen Sie mit **SAVE**.

  Network Address Translation ist für die ausgewählte Schnittstelle bzw. den ausgewählten WAN-Partner aktiviert.
- Verlassen Sie ***IP*** ➧ ***NETWORK ADDRESS TRANSLATION*** mit **EXIT**.
- Verlassen Sie ***IP*** mit **EXIT**.

  Sie befinden sich wieder im Hauptmenü und haben einen WAN-Partner eingerichtet.

6.2.2 Mit BinGO! ins Internet

Beispiele Im Anschluß an die in Kapitel 6.2.1, Seite 152 beschriebene allgemeine Vorgehensweise, nach der Sie prinzipiell für jeden Internet Service Provider (ISP) vorgehen können, sind hier einige Beispiele angegeben. Sie zeigen, wie Sie Ihren Internetzugang mit bestimmten Providern schnell und einfach einrichten:

- Beispiel 1: T-Online
- Beispiel 2: Compuserve

Legen Sie sich die Zugangsdaten, die Sie von Ihrem ISP erhalten haben, zurecht (siehe Kapitel 3.2.1, Seite 40). Die Bezeichnungen können unter Umständen von Provider zu Provider leicht variieren.

Los geht's:

Beispiel 1: T-Online

Wenn Sie Ihren Internetzugang über den Provider T-Online herstellen wollen, gehen Sie folgendermaßen vor:

WAN-Partner einrichten

- Gehen Sie zu ***WAN PARTNER*** ➧ **ADD**.
- Geben Sie *Partner Name* (= Providername) ein: *T_ONLINE*.
- Wählen Sie *Encapsulation* aus: *PPP*.
- Wählen Sie *Compression* aus: *none*.
- Wählen Sie *Encryption* aus: *none*.

Rufnummer eintragen

- Wählen Sie *WAN Numbers* aus und bestätigen Sie mit der **Eingabetaste**.
- Fügen Sie einen neuen Eintrag mit **ADD** hinzu.
- Geben Sie *Number* (= Einwahlnummer) ein, z. B. *0191011*.
- Wählen Sie *Direction* aus: *outgoing*.
- Bestätigen Sie mit **SAVE**.

  Die Rufnummer, mit der Sie sich bei T-Online einwählen, steht nun in der Liste.
- Verlassen Sie ***WAN PARTNER*** ➧ **ADD** ➧ ***WAN NUMBERS*** mit **EXIT**.

PPP-Authentisierung festlegen

- Wählen Sie *PPP* aus und bestätigen Sie mit der **Eingabetaste**.
- Wählen Sie *Authentication* aus: *CHAP + PAP*.
- Geben Sie *Local PPP ID* (=Anschlußkennung + T-Online-Nummer + Mitbenutzerkennung) ein, z. B. *123456789012081512345678#0001*.
- Geben Sie *PPP Password* (=Paßwort) ein.
- Deaktivieren Sie *Keepalives: off*.
- Deaktivieren Sie *Link Quality Monitoring: off*.

- Bestätigen Sie mit **OK**.
  Sie befinden sich wieder im Menü ***WAN PARTNER*** ➧ **ADD**.

Shorthold festlegen

- Wählen Sie *Advanced Settings* aus und bestätigen Sie mit der **Eingabetaste**.
- Wählen Sie *Callback* aus: *no*.
- Geben Sie *Static Short Hold (sec)* ein, z. B. *60*.
- Geben Sie *Idle for Dynamic Short Hold (%)* ein, z. B. *0*.
- Geben Sie *Delay after Connection Failure (sec)* ein, z. B. *300*.
- Wählen Sie *Channel-Bundling* aus: *no*.
- Wählen Sie *Layer 1 Protocol* aus: *ISDN 64 kbps*.
- Bestätigen Sie mit **OK**.
  Sie befinden sich wieder im Menü ***WAN PARTNER*** ➧ **ADD**.

IP-Konfiguration durchführen

- Wählen Sie *IP* aus und bestätigen Sie mit der **Eingabetaste**.
- Wählen Sie *IP Transit Network* aus: *dynamic client*.
- Wählen Sie *Advanced Settings* aus und bestätigen Sie mit der **Eingabetaste**.
- Wählen sie *RIP Send: none*.
- Wählen Sie *RIP Receive: none*.
- Aktivieren Sie *Van Jacobson Header Compression: on*.
- Wählen Sie *Dynamic Name Server Negotiation* aus: *client (receive)*.
- Deaktivieren Sie *IP Accounting: off*.
- Deaktivieren Sie *Back Route Verify: off*.
- Wählen Sie *Route Announce* aus: *up or dormant*.
- Wählen Sie *Proxy Arp* aus: *off*.
- Bestätigen Sie mit **OK**.
- Bestätigen Sie mit **SAVE**.
- Bestätigen Sie erneut mit **SAVE**.
- Verlassen Sie ***WAN PARTNER*** mit **EXIT**.

Routing-Eintrag erstellen

- Gehen Sie zu ***IP*** ➧ ***ROUTING***.
- Fügen Sie einen neuen Eintrag mit **ADD** hinzu.
- Wählen Sie *Route Type* aus: *Default route*.
- Wählen Sie *Network* aus: *WAN without transit network*.
- Wählen Sie *Partner / Interface* aus: *T_Online*.
- Geben Sie *Metric* ein, z. B. *1*.
- Bestätigen Sie mit **SAVE**.
- Verlassen Sie ***IP*** ➧ ***ROUTING*** mit **EXIT**.

NAT aktivieren

- Gehen Sie zu ***IP*** ➧ ***NETWORK ADDRESS TRANSLATION***.
- Wählen Sie das IP Interface T_Online aus und bestätigen Sie mit der **Eingabetaste**.
- Wählen Sie *Network Address Translation* aus: *on*.
- Bestätigen Sie mit **SAVE**.
- Verlassen Sie ***IP*** ➧ ***NETWORK ADDRESS TRANSLATION*** mit **EXIT**.
- Verlassen Sie ***IP*** mit **EXIT**.

  Sie befinden sich wieder im Hauptmenü.

  Die Konfiguration des Internetzugangs über T-Online ist abgeschlossen.

Beispiel 2: Compuserve

Wenn Sie Ihren Internetzugang über den Provider Compuserve herstellen wollen, gehen Sie folgendermaßen vor:

Hier wird der Zugang zu Compuserve über direkte Einwahl auf einen Compuserve Netzwerk-Knoten beschrieben.

Wenn Sie Compuserve indirekt über T-Onlines Compuserve Gateway erreichen wollen, ersetzen Sie an entsprechender Stelle die Konfigurationsschritte durch die folgenden Eintragungen:

- Wählen Sie *Encapsulation* aus: *Async PPP over X.75/T.70/BTX*.
- Geben Sie *Number* ein: *01910*.
- Wählen Sie *Provider* aus: *Compuserve via T-Online*.

WAN-Partner einrichten

- Gehen Sie zu ***WAN PARTNER*** ➧ **ADD**.
- Geben Sie *Partner Name* (= Providername) ein: *COMPUSERVE*.
- Wählen Sie *Encapsulation* aus: *Async PPP over X.75*.
- Wählen Sie *Compression* aus: *none*.
- Wählen Sie *Encryption* aus: *none*.

Rufnummer eintragen

- Wählen Sie *WAN Numbers* aus und bestätigen Sie mit der **Eingabetaste**.
- Fügen Sie einen neuen Eintrag mit **ADD** hinzu.
- Geben Sie *Number* (= Einwahlnummer) ein.
- Wählen Sie *Direction* aus: *outgoing*.
- Bestätigen Sie mit **SAVE**.

  Die Rufnummer, mit der Sie sich bei Compuserve einwählen, steht nun in der Liste.
- Verlassen Sie ***WAN PARTNER*** ➧ **ADD** ➧ ***WAN NUMBERS*** mit **EXIT**.

PPP-Authentisierung festlegen

- Wählen Sie *PPP* aus und bestätigen Sie mit der **Eingabetaste**.
- Wählen Sie *Authentication* aus: *none*.
- Deaktivieren Sie *Keepalives: off*.
- Deaktivieren Sie *Link Quality Monitoring: off*.
- Bestätigen Sie mit **OK**.

  Sie befinden sich wieder im Menü ***WAN PARTNER*** ➧ **ADD**.

Shorthold festlegen

- Wählen Sie *Advanced Settings* aus und bestätigen Sie mit der **Eingabetaste**.
- Wählen Sie *Callback* aus: *no*.
- Geben Sie *Static Short Hold (sec)* ein, z. B. *120*.
- Geben Sie *Idle for Dynamic Short Hold (%)* ein, z. B. *0*.
- Geben Sie *Delay after Connection Failure (sec)* ein, z. B. *300*.
- Wählen Sie *Channel-Bundling* aus: *no*.
- Wählen Sie *Layer 1 Protocol* aus: *ISDN 64 kbps*.

Authentisierung festlegen

- Wählen Sie *Provider Configuration* aus und bestätigen Sie mit der **Eingabetaste**.
- Wählen Sie *Provider* aus: *Compuserve Network*.
- Geben Sie *Host* ein: *CIS*.
- Geben Sie *User ID* (= Ihr Benutzername) ein.
- Geben Sie *Password* (=Paßwort) ein.
- Bestätigen Sie mit **OK**.
- Bestätigen Sie erneut mit **OK**.
  Sie befinden sich wieder im Menü ***WAN PARTNER*** ➧ **ADD**.

IP-Konfiguration durchführen

- Wählen Sie *IP* aus und bestätigen Sie mit der **Eingabetaste**.
- Wählen Sie *IP Transit Network* aus: *dynamic client*.
- Wählen Sie *Advanced Settings* aus und bestätigen Sie mit der **Eingabetaste**.
- Wählen sie *RIP Send: none*.
- Wählen Sie *RIP Receive: none*.
- Deaktivieren Sie *Van Jacobson Header Compression: off*.
- Wählen Sie *Dynamic Name Server Negotiation* aus: *client (receive)*.
- Deaktivieren Sie *IP Accounting: off*.
- Deaktivieren Sie *Back Route Verify: off*.
- Wählen Sie *Route Announce* aus: *up or dormant*.
- Wählen Sie *Proxy Arp* aus: *off*.
- Bestätigen Sie mit **OK**.
- Bestätigen Sie mit **SAVE**.
- Bestätigen Sie erneut mit **SAVE**.
- Verlassen Sie ***WAN PARTNER*** mit **EXIT**.

Routing-Eintrag erstellen

- Gehen Sie zu ***IP*** ➧ ***ROUTING***.
- Fügen Sie einen neuen Eintrag mit **ADD** hinzu.

- Wählen Sie *Route Type* aus: *Default route*.
- Wählen Sie *Network* aus: *WAN without transit network*.
- Wählen Sie *Partner / Interface* aus: *COMPUSERVE*.
- Geben Sie *Metric* ein, z. B. *1*.
- Bestätigen Sie mit **SAVE**.
- Verlassen Sie ***IP*** ➧ ***ROUTING*** mit **EXIT**.

NAT aktivieren

- Gehen zu ***IP*** ➧ ***NETWORK ADDRESS TRANSLATION***.
- Wählen Sie das IP Interface COMPUSERVE aus und bestätigen Sie mit der **Eingabetaste**.
- Wählen Sie *Network Address Translation* aus: *on*.
- Bestätigen Sie mit **SAVE**.
- Verlassen Sie ***IP*** ➧ ***NETWORK ADDRESS TRANSLATION*** mit **EXIT**.
- Verlassen Sie ***IP*** mit **EXIT**.

  Sie befinden sich wieder im Hauptmenü.

  Die Konfiguration des Internetzugangs über Compuserve ist abgeschlossen.

6.2.3 BinGO! ans Firmennetz anbinden

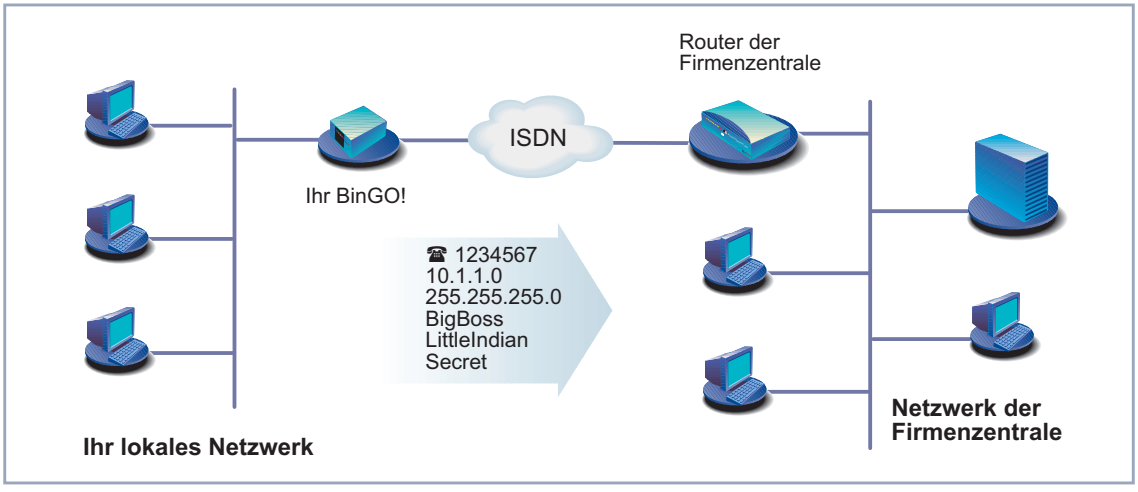


Bild 6-6: **BinGO!** und Ihre Firmenzentrale

In diesem Kapitel ist eine schnelle Konfiguration für eine Firmennetzanbindung (LAN-LAN-Kopplung) mit **BinGO!** Schritt für Schritt dargestellt. Legen Sie sich die Daten zurecht, die Sie vom System-Administrator der Firmenzentrale erhalten haben (siehe auch Kapitel 3.2.1, Seite 40). Wenn Sie sich an manchen Stellen nicht sicher sind, beachten Sie Kapitel 6.2.1, Seite 152.

Gehen Sie folgendermaßen vor:

WAN-Partner einrichten

- Gehen Sie zu ***WAN PARTNER*** ➧ **ADD**.
- Geben Sie *Partner Name* (= Kennung der Firmenzentrale) ein, z. B. *BigBoss*.
- Wählen Sie *Encapsulation* aus: *PPP*.
- Wählen Sie *Compression* aus: *STAC*.
- Wählen Sie *Encryption* aus: *none*.

Rufnummer eintragen

- Wählen Sie *WAN Numbers* aus und bestätigen Sie mit der **Eingabetaste**.
- Fügen Sie einen neuen Eintrag mit **ADD** hinzu.

- Geben Sie *Number* (= Rufnummer des Routers der Firmenzentrale) ein, z. B. *0911987654321*.
- Wählen Sie *Direction* aus: *outgoing*.
- Bestätigen Sie mit **SAVE**.

  Die Rufnummer, mit der Sie sich bei der Firmenzentrale einwählen, steht nun in der Liste.
- Verlassen Sie ***WAN PARTNER*** ➧ **ADD** ➧ ***WAN NUMBERS*** mit **EXIT**.

PPP-Authentisierung festlegen

- Wählen Sie *PPP* aus und bestätigen Sie mit der **Eingabetaste**.
- Wählen Sie *Authentication* aus: *CHAP + PAP*.
- Geben Sie *Partner PPP ID* (=Kennung der Firmenzentrale) ein, z. B. *BigBoss*.
- Geben Sie *Local PPP ID* (=Ihre eigene Kennung) ein, z. B. *LittleIndian*.
- Geben Sie *PPP Password* (=Gemeinsames Paßwort für diese Verbindung) ein.
- Deaktivieren Sie *Keepalives: off*.
- Deaktivieren Sie *Link Quality Monitoring: off*.
- Bestätigen Sie mit **OK**.

  Sie befinden sich wieder im Menü ***WAN PARTNER*** ➧ **ADD**.

Shorthold festlegen

- Wählen Sie *Advanced Settings* aus und bestätigen Sie mit der **Eingabetaste**.
- Wählen Sie *Callback* aus: *no*.
- Geben Sie *Static Short Hold (sec)* ein, z. B. *20*.
- Geben Sie *Idle for Dynamic Short Hold (%)* ein, z. B. *0*.
- Geben Sie *Delay after Connection Failure (sec)* ein, z. B. *300*.
- Wählen Sie *Channel-Bundling* aus: *no*.
- Wählen Sie *Layer 1 Protocol* aus: *ISDN 64 kbps*.
- Bestätigen Sie mit **OK**.

  Sie befinden sich wieder im Menü ***WAN PARTNER*** ➧ **ADD**.

IP-Konfiguration durchführen

- Wählen Sie *IP* aus und bestätigen Sie mit der **Eingabetaste**.
- Wählen Sie *IP Transit Network* aus: *no*.
- Geben Sie *Partner's LAN IP Address* (= Netzadresse der Firmenzentrale) ein: z. B. *10.1.1.0.*
- Geben Sie *Partner's LAN Netmask* (= Netzmaske der Firmenzentrale) ein: z. B. *255.255.255.0.*
- Wählen Sie *Advanced Settings* aus und bestätigen Sie mit der **Eingabetaste**.
- Wählen sie *RIP Send: none*.
- Wählen Sie *RIP Receive: none*.
- Aktivieren Sie *Van Jacobson Header Compression: off*.
- Wählen Sie *Dynamic Name Server Negotiation* aus: *yes* (wenn Sie Internetzugang konfiguriert haben) oder *off* (wenn Sie keinen Internetzugang konfiguriert haben).
- Aktivieren Sie *IP Accounting: on*.
- Aktivieren Sie *Back Route Verify: on*.
- Wählen Sie *Route Announce* aus: *up or dormant*.
- Wählen Sie *Proxy Arp* aus: *off*.
- Bestätigen Sie mit **OK**.
- Bestätigen Sie mit **SAVE**.
- Bestätigen Sie erneut mit **SAVE**.
- Verlassen Sie ***WAN PARTNER*** mit **EXIT**.

  Sie befinden sich wieder im Hauptmenü.

  Die Konfiguration des Zugangs zur Firmennetzzentrale ist abgeschlossen.

Routing-Eintrag erstellen

Wenn Sie keinen Internetzugang eingerichtet haben, dann können Sie für den Zugang zur Firmenzentrale eine Default-Route einrichten (siehe Kapitel 6.2.1, Seite 152):

- Machen Sie dazu in ***IP*** ➧ ***ROUTING*** ➧ **ADD** folgende Eintragungen:
  - *Route Type: Default route*
  - *Network: WAN without transit network*
  - *Partner / Interface:* z. B. *BigBoss*
  - *Metric:* z. B. *1*

Wenn das Netzwerk der Firmenzentrale aus mehreren LANs besteht (Subnetze) und Sie keine Default-Route zur Firmenzentrale einrichten, dann müssen Sie für jedes LAN, das Sie erreichen wollen, einen eigenen Routing-Eintrag erstellen. Beachten Sie dazu die Hinweise in Kapitel 6.2.1, Seite 152 und Bild 6-5, Seite 174.

- Wiederholen Sie die Schritte für das Erstellen eines Routing-Eintrags so oft, bis Sie alle notwendigen Routen eingetragen haben.

- Bestätigen Sie mit **SAVE**.
- Verlassen Sie ***IP*** ➧ ***ROUTING*** mit **EXIT**.
- Verlassen Sie ***IP*** mit **EXIT**.

6.3 Konfigurationsdatei sichern

Nachdem Sie nun auf **BinGO!** eine funktionierende Konfiguration erstellt haben, sollten Sie diese sichern:

- Wählen Sie im Setup Tool Hauptmenü **Exit** aus und bestätigen Sie mit der **Eingabetaste**.

  Ein weiteres Menüfenster erscheint:

```
BinGO! Setup Tool                                BinTec Communications AG
[EXIT]: Exit Setup                                               MyBinGO!


            Back to Main Menu

            Save as boot configuration and exit
            Exit without saving
```

Sie haben drei Möglichkeiten:

- Wählen Sie **Back to Main Menu**, um zum Hauptmenü des Setup Tools zurückzukehren.
- Wählen Sie **Save as boot configuration and exit**, um die Konfigurationsdaten als Datei boot im Flash-Speicher abzuspeichern.

  Es erscheint die SNMP-Shell von **BinGO!** mit dem Login-Prompt. Alle Änderungen, die Sie vorher mit dem Setup Tool durchgeführt haben, sind gesichert. Beim nächsten Starten von **BinGO!** wird die so abgespeicherte Konfigurationsdatei geladen.
- Wählen Sie **Exit without saving**, um das Setup Tool zu verlassen, die vorgenommenen Änderungen aber nicht zu speichern.

  Es erscheint die SNMP-Shell von **BinGO!** mit dem Login-Prompt. Alle Änderungen, die Sie vorher mit dem Setup Tool durchgeführt haben, gehen beim Ausschalten von **BinGO!** verloren.

7 Weiterführende Konfiguration

In diesem Kapitel finden Sie weitere Möglichkeiten zur Konfiguration von **BinGO!** für den fortgeschrittenen Benutzer. Wenn Sie zusätzliche Einstellungen machen wollen, die mit dem Configuration Wizard bzw. dem Kapitel 6, Seite 123 nicht abgedeckt werden, dann sind Sie hier richtig.

Folgende Konfigurationsschritte werden erläutert:

- Allgemeine ➤➤ **WAN**-Einstellungen
- WAN-Partner-spezifische Einstellungen
- Grundlegende ➤➤ **IP**-Einstellungen
- ➤➤ **IPX**-Einstellungen
- Funktionen mit Zusatzlizenz

7.1 Allgemeine WAN-Einstellungen

Allgemeine WAN-Funktionen:

- **BinGO!** als dynamischer IP-Adreß-➤➤ **Server**
- ➤➤ **CAPI** User Concept
- Taschengeldkonto
- Allgemeine ➤➤ **PPP**-Einstellungen

Diese Einstellungen sind nicht an bestimmte WAN-Partner gekoppelt, Sie betreffen alle ➤➤ **ISDN**-Verbindungen.

7.1.1 Dynamic IP Address Server

IP-Adreß-Pools

BinGO! kann als dynamischer IP-Adreß-Server für PPP-Verbindungen agieren. Dafür stellen Sie einen oder mehrere Pools von ➤➤ **IP-Adressen** zur Verfügung. Diese IP-Adressen können für die Dauer der Verbindung an einen einwählenden WAN-Partner vergeben werden.

Eingetragene Host-Routen haben immer Vorrang vor IP-Adressen aus den Adreß-Pools. D. h. wenn ein eingehender Ruf authentisiert wurde, überprüft **BinGO!** zunächst, ob für den Anrufer in der Routing-Tabelle eine Host-Route eingetragen ist. Wenn dies nicht der Fall ist, kann **BinGO!** eine IP-Adresse aus einem Adreß-Pool zuweisen (falls verfügbar).

Bei Adreß-Pools mit mehr als einer IP-Adresse können Sie nicht festlegen, welcher WAN-Partner welche Adresse bekommt. Die Adressen werden zunächst einfach der Reihe nach vergeben. Bei einer erneuten Einwahl innerhalb eines Intervalls von einer Stunde wird aber versucht, wieder die zuletzt an diesen Partner vergebene IP-Adresse zuzuweisen.

Die Konfiguration erfolgt in:

- ***IP*** ➧ ***Dynamic IP Addresses (Server Mode)***
- ***WAN Partner*** ➧ ***Edit*** ➧ ***IP***
- ***WAN Partner*** ➧ ***Edit*** ➧ ***IP*** ➧ ***Advanced Settings***

Feld	Bedeutung
Pool ID	Eindeutige Nummer zur Identifizierung des Adreß-Pools. Ein Pool kann sich aus mehreren Adressbereichen zusammensetzen.
IP Address	Erste IP-Adresse des Adreß-Pools.
Number of consecutive addresses	Anzahl der IP-Adressen im Adreß-Pool, einschließlich der ersten IP-Adresse (*IP Address*).

Tabelle 7-1: ***IP*** ➧ ***DYNAMIC IP ADDRESSES (SERVER MODE)***

Feld	Bedeutung
IP Transit Network	Legt fest, ob zwischen **BinGO!** und LAN des WAN-Partners ein Transit-Netzwerk verwendet werden soll. Bei Zuweisung eines Adreß-Pools muß hier *dynamic server* ausgewählt werden.

Tabelle 7-2: ***WAN PARTNER*** ➧ ***EDIT*** ➧ ***IP***

Feld	Bedeutung
IP Address Pool	*Pool ID* des dem WAN-Partner zugewiesenen Adreß-Pools.

Tabelle 7-3: ***WAN PARTNER*** ➧ ***EDIT*** ➧ ***IP*** ➧ ***ADVANCED SETTINGS***

ToDo Gehen Sie folgendermaßen vor:

- Gehen Sie zu ***IP*** ➧ ***DYNAMIC IP ADDRESSES (SERVER MODE)*** ➧ **ADD**.
- Geben Sie *Pool ID* ein.
- Geben Sie *IP Address* ein.
- Geben Sie *Number of consecutive addresses* ein.
- Bestätigen Sie mit **SAVE**.

- Gehen Sie zu ***WAN PARTNER*** ➧ ***EDIT*** ➧ ***IP***, um einem WAN-Partner einen Adreß-Pool zuzuweisen.
- Wählen Sie *IP Transit Network* aus: *dynamic server*.
- Gehen Sie zu ***WAN PARTNER*** ➧ ***EDIT*** ➧ ***IP*** ➧ ***ADVANCED SETTINGS***.
- Geben Sie *IP Address Pool* ein: *Pool ID*.
- Bestätigen Sie mit **OK**.
- Bestätigen Sie mit **SAVE**.

7.1.2 CAPI User Concept

Benutzername und Paßwort

Das CAPI User Concept erlaubt eine Kontrolle über den Zugriff auf den ➧➧ **CAPI**-Dienst. Damit wird erreicht, daß nur Benutzer, die mit Benutzernamen und Paßwort eingetragen sind, die CAPI-Dienste von **BinGO!** nutzen können.

Beispiel

Damit wird z. B. ermöglicht, daß ein eingehendes Fax an den Benutzer Winnetou auch wirklich nur an den Benutzer Winnetou und nicht etwa den Benutzer OldShatterhand, der sich im gleichen LAN befindet, weitergeleitet wird. Wenn das CAPI User Concept nicht genutzt wird (siehe Kapitel 6.1.4, Seite 133), werden alle eingehenden Rufe, die an den Dienst CAPI weitergeleitet werden, allen CAPI-Applikationen im LAN angeboten. Und wer am schnellsten reagiert, erhält den Ruf. Wenn OldShatterhand also schneller ist...

Die Konfiguration erfolgt in:

- ***CAPI*** ➧ ***USER***
- ***CM-1BRI, ISDN S0*** ➧ ***INCOMING CALL ANSWERING***

Feld	Bedeutung
Name	Benutzername, für den Zugriff auf den CAPI-Dienst erlaubt bzw. gesperrt werden soll (maximal 16 Zeichen).
Password	Paßwort, mit dem sich der Benutzer *Name* identifizieren muß, um Zugang zum CAPI-Dienst zu erhalten.
CAPI	Legt fest, ob Zugriff auf den CAPI-Dienst für den Benutzer *Name* erlaubt oder gesperrt wird. Mögliche Werte: ■ *enabled:* Zugriff auf CAPI erlaubt ■ *disabled:* Zugriff auf CAPI gesperrt

Tabelle 7-4: ***CAPI*** ➧ ***USER***

Feld	Bedeutung
Item	Dienst, dem ein Ruf auf die untenstehende *Number* zugewiesen werden soll.
Number	Rufnummer, unter der der oben eingetragene Dienst (*Item*) erreicht werden kann.
Mode	Modus, mit dem **BinGO!** den Ziffernvergleich von *Number* mit der Called Party Number des eingehenden Rufes durchführt: *right to left:* Dies ist der Standard. *left to right (DDI):* Immer dann auswählen, wenn **BinGO!** mit einem Point-to-Point-Anschluß (Anlagenanschluß) verbunden ist.
Username	Entspricht *Name* in ***CAPI*** ➧ ***USER***. Benutzer, an den ein eingehender Ruf an den Dienst CAPI unter *Number* weitergeleitet werden soll.
Bearer	Art des eingehenden Rufes. Mögliche Werte: ■ *data:* Daten-Ruf ■ *voice:* Sprach-Ruf ■ *any:* entweder Daten- oder Sprach-Ruf

Tabelle 7-5: ***CM-1BRI, ISDN S0*** ➧ ***INCOMING CALL ANSWERING***

Wenn sich beim Starten von **BinGO!** in ***CAPI*** ➧ ***USER*** kein Eintrag befindet, wird automatisch ein Standard-Eintrag ohne Paßwort erzeugt (mit *Name* = *default* und *CAPI* = *enabled*).

ToDo Gehen Sie folgendermaßen vor:

➤ Gehen Sie zu ***CAPI*** ➧ ***USER***.

➤ Wählen Sie einen bestehenden Eintrag aus und bestätigen Sie mit der **Eingabetaste** oder fügen Sie einen neuen Eintrag mit **ADD** hinzu.

➤ Geben Sie *Name* ein.

- Geben Sie *Password* ein.
- Wählen Sie *CAPI* aus.
- Bestätigen Sie mit **SAVE**.
- Wiederholen Sie diese Schritte für jeden Benutzer im LAN.
- Gehen Sie zu ***CM-1BRI, ISDN S0*** ➧ ***INCOMING CALL ANSWERING***.

  Machen Sie hier für jeden Benutzer im LAN, der Zugriff auf den Dienst CAPI hat, einen Eintrag.
- Wählen Sie einen bestehenden Eintrag aus und bestätigen Sie mit der **Eingabetaste** oder fügen Sie einen neuen Eintrag mit **ADD** hinzu.
- Wählen Sie *Item* aus: *CAPI*.

Falls Sie auf Ihrem Rechner mit einer Kommunikationsanwendung arbeiten, die auf Remote-CAPI 1.1 aufsetzt (aktuell: Remote-CAPI 2.0), muß **BinGO!** die ➤➤ **MSN**s (=*Number*, mehrstellig) des eingehenden Rufes in ➤➤ **EAZ**s (einstellig) übersetzen (CAPI 1.1 kann nur einstellige Nummern unterscheiden). Deswegen heißt der CAPI-Eintrag unter *Item* nicht einfach *"CAPI"*, sondern *"CAPI 1.1 EAZ x Mapping"*.
Achten Sie bei CAPI 1.1 also darauf, jede *Number* auf eine eigene EAZ zu "mappen". Wählen Sie also z. B. für *Number = 1234* den Eintrag *Item = CAPI 1.1 EAZ **0** Mapping* und für *Number = 5678* den Eintrag *Item = CAPI 1.1 EAZ **1** Mapping*.

Bei CAPI 2.0 wird die MSN direkt ausgewertet, eine "Übersetzung" zu EAZ ist nicht notwendig, Sie können für jede Number den gleichen CAPI 1.1 EAZ x Mapping-Eintrag verwenden.

- Geben Sie *Number* ein.
- Wählen Sie *Mode* aus.
- Geben Sie *Username* ein.
- Wählen Sie *Bearer* aus.
- Bestätigen Sie mit **SAVE**.
- Wiederholen Sie diese Schritte so oft, bis Sie für jeden Nutzer einen Eintrag erstellt haben.

7.1.3 Taschengeldkonto (Credits Based Accounting System)

ISDN-Gebühren

Das Taschengeldkonto von **BinGO!** unterstützt Sie dabei, den Überblick über anfallende ISDN-Gebühren nicht zu verlieren. Es ermöglicht Ihnen, festzulegen, wieviele Verbindungen in einem bestimmten Zeitraum maximal anfallen dürfen. Sie können für jedes Subsystem (➤➤ **PPP**, ➤➤ **CAPI**, ➤➤ **ISDN-Login**) Einstellungen vornehmen bezüglich der Anzahl der Verbindungen, der Verbindungszeit und der anfallenden Gebühren. Ist das festgelegte Limit überschritten, kann **BinGO!** innerhalb des festgelegten Zeitraums keine Verbindungen mehr aufbauen. So können Sie Konfigurationsfehler rechtzeitig erkennen, bevor Ihre Telefonrechnung sehr hoch ausfällt!

Syslog-Messages

Syslog-Messages werden erzeugt bei Erreichen von 90% bzw. 100% des Limits und wenn eine Verbindung vom Taschengeldkonto wegen überschrittenem Limit verhindert wird.

Nach Aus- und wieder Einschalten bzw. Rebooten von **BinGO!** steht Ihnen wieder das gesamte Konto zur Verfügung.

Die Konfiguration erfolgt in ***ISDN*** ➧ ***CREDITS***:

Feld	Bedeutung
Surveillance	Definiert, ob das Taschengeldkonto für das jeweilige Subsystem aktiviert werden soll. Mögliche Werte: *off*, *on*. Bei *on*, können Sie die im Folgenden aufgelisteten Parameter festlegen.
Measure Time (sec)	Zeitraum in Sekunden, für den das Limit gilt.
Maximum Number of Incoming Connections	Anzahl der erlaubten eingehenden Verbindungen während *Measure Time (sec)*. Wenn Sie diese Einstellung mit *on* aktivieren, können Sie den gewünschten Wert in der darunterliegenden Zeile eintragen.
Maximum Number of Outgoing Connections	Anzahl der erlaubten ausgehenden Verbindungen während *Measure Time (sec)*. Wenn Sie diese Einstellung mit *on* aktivieren, können Sie den gewünschten Wert in der darunterliegenden Zeile eintragen.
Maximum Charge	Maximal erlaubte Gebühreneinheiten während *Measure Time (sec)*. Wenn Sie diese Einstellung mit *on* aktivieren, können Sie den gewünschten Wert in der darunterliegenden Zeile eintragen.
Maximum Time for Incoming Connections (sec)	Maximal erlaubter Zeitraum in Sekunden für eingehende Verbindungen während *Measure Time (sec)*. Wenn Sie diese Einstellung mit *on* aktivieren, können Sie den gewünschten Wert in der darunterliegenden Zeile eintragen.

Feld	Bedeutung
Maximum Time for Outgoing Connections (sec)	Maximal erlaubter Zeitraum in Sekunden für ausgehende Verbindungen während *Measure Time (sec)*. Wenn Sie diese Einstellung mit *on* aktivieren, können Sie den gewünschten Wert in der darunterliegenden Zeile eintragen.

Tabelle 7-6: ***ISDN*** ➧ ***CREDITS***

ToDo Gehen Sie folgendermaßen vor:

- Gehen Sie zu ***ISDN*** ➧ ***CREDITS***.
- Wählen Sie *Subsystem* aus und bestätigen Sie mit der **Eingabetaste**.
- Wählen Sie *Surveillance* aus: *on*, wenn Sie das Taschengeldkonto für das gewählte *Subsystem* nutzen wollen.
- Geben Sie *Measure Time (sec)* ein, z. B. *86400* (= 24 Stunden).
- Aktivieren Sie gegebenenfalls *Maximum Number of Incoming Connections* und tragen Sie gegebenenfalls den gewünschten Wert ein.
- Aktivieren Sie gegebenenfalls *Maximum Number of Outgoing Connections* und tragen Sie gegebenenfalls den gewünschten Wert ein.
- Aktivieren Sie gegebenenfalls *Maximum Charge* und tragen Sie gegebenenfalls den gewünschten Wert ein.
- Aktivieren Sie gegebenenfalls *Maximum Time for Incoming Connections (sec)* und tragen Sie gegebenenfalls den gewünschten Wert ein.
- Aktivieren Sie gegebenenfalls *Maximum Time for Outgoing Connections (sec)* und tragen Sie gegebenenfalls den gewünschten Wert ein.
- Bestätigen Sie mit **SAVE**.

7.1.4 Allgemeine PPP-Einstellungen

Authentisierung ➧➧ **PPP**-Einstellungen, die z. B. zur Authentisierung der Verbindungspartner mit ➧➧ **CHAP** oder ➧➧ **PAP** erforderlich sind, tragen Sie bei jedem WAN-

Partner ein (siehe Kapitel 6.2.1, Seite 152). Wenn ein Ruf eingeht, erkennt **BinGO!** dann anhand der Calling Party's Number mit Hilfe von ➤➤ **CLID** (Calling Line Identification) den anrufenden WAN-Partner und weiß damit, welche Authentisierungsverhandlungen er mit diesem vereinbart hat. Wenn die Authentisierung klappt, wird der Ruf angenommen.

CLID

In manchen Fällen kann ein eingehender Ruf aber nicht via CLID identifiziert werden. Dies ist z. B. dann der Fall,

- wenn der Ruf über eine analoge Leitung erfolgt (der Anrufer wählt sich per ➤➤ **Modem** auf Ihrem Router ein).
- wenn mit dem anrufenden WAN-Partner das Authentisierungsprotokoll MS-CHAP festgelegt wurde.

In beiden Fällen kommt bei **BinGO!** keine Calling Line Number an. Eine Identifizierung des Anrufers via CLID kann also nicht erfolgen, auch wenn der Anrufer als WAN-Partner eingetragen ist. **BinGO!** weiß nicht, mit welchem ➤➤ **PPP-Authentisierung**sprotokoll er den eingehenden Ruf identifizieren kann.

Allgemeine PPP-Einstellungen

Um eine Rufannahme trotzdem zu ermöglichen, führt **BinGO!** mit dem Anrufer das PPP-Authentisierungsprotokoll durch, das allgemein festgelegt wurde, sich also nicht auf einen bestimmten WAN-Partner bezieht. Wenn die mit Hilfe des ausgeführten Authentisierungsprotokolls erhaltenen Daten, wie z. B. Paßwort, mit den Daten eines eingetragenen WAN-Partners übereinstimmen, nimmt **BinGO!** den Ruf an.

Die Konfiguration der allgemeinen PPP-Einstellungen erfolgt in ***PPP:***

Feld	Bedeutung
Authentication Protocol	Definiert das PPP-Authentisierungs-Protokoll, das dem Anrufer als erstes angeboten wird. Mögliche Werte: ■ *PAP:* nur PAP ■ *CHAP:* nur CHAP ■ *CHAP + PAP:* erst CHAP, dann PAP ■ *MS-CHAP:* nur MS-CHAP ■ *CHAP + PAP + MS-CHAP:* erst CHAP, bei Ablehnung anschließend das vom WAN-Partner gewollte Protokoll ■ *none:* keine PPP-Authentisierung
Radius Server Authentication	Auf **BinGO!** nicht verfügbar.
PPP Link Quality Monitoring	Definiert, ob Link Quality Monitoring für PPP-Verbindungen durchgeführt wird. Mögliche Werte: ■ *no*, wird nicht durchgeführt. ■ *yes*, die Verbindungsstatistiken werden in der ➤➤ **MIB**-Tabelle **biboPPPLQMTable** gespeichert.

Tabelle 7-7: ***PPP***

ToDo Gehen Sie folgendermaßen vor, um die allgemeinen PPP-Einstellungen festzulegen:

➤ Gehen Sie zu ***PPP***.

➤ Wählen Sie *Authentication Protocol* aus, z. B. *CHAP + PAP + MS-CHAP*.

➤ Wählen Sie *Link Quality Monitoring aus*, z. B. *no*.

7.2 WAN-Partner-spezifische Einstellungen

Spezielle Funktionen für ➤➤ **WAN-Partner** ermöglichen, die Eigenschaften für Verbindungen zu WAN-Partnern individuell festzulegen. Die beschriebenen Konfigurationsschritte nehmen Sie für jeden WAN-Partner separat vor.

- Delay after Connection Failure
- Channel-Bundling
- Layer 1 Protocol
- IP Transit Network
- Übermittlung von DNS- und WINS-Server-IP-Adressen an WAN-Partner
- ➤➤ **RIP**
- Komprimierung: ➤➤ **VJHC**, ➤➤ **STAC**, MS-STAC
- ➤➤ **Proxy ARP**

Im Folgenden werden die jeweils erforderlichen Konfigurationsschritte genau erläutert.

7.2.1 Delay after Connection Failure

Mit dieser Funktion richten Sie eine Verzögerung nach einem Fehler im Verbindungsaufbau ein.

Die Konfiguration erfolgt in ***WAN Partner*** ➧ ***Edit*** ➧ ***Advanced Settings***:

Feld	Bedeutung
Delay after Connection Failure (sec)	Blocktimer. Gibt an, für wie viele Sekunden nach einem Fehler im Verbindungsaufbau keine erneute Einwahl auf **BinGO!** erfolgen kann.

Tabelle 7-8: ***WAN Partner*** ➧ ***Edit*** ➧ ***Advanced Settings***

ToDo Gehen Sie folgendermaßen vor:

- Gehen Sie zu ***WAN Partner*** ➧ ***Edit*** ➧ ***Advanced Settings***.
- Geben Sie *Delay after Connection Failure (sec)* ein.
- Bestätigen Sie mit **OK**.
- Bestätigen Sie mit **SAVE**.

7.2.2 Channel Bundling

BinGO! unterstützt dynamische und statische ➤➤ **Kanalbündelung**.

Dynamisch Dynamische Kanalbündelung bedeutet, daß **BinGO!** bei Bedarf, also bei großen Datenmengen, den zweiten ➤➤ **ISDN**-B-Kanal für Verbindungen mit dem WAN-Partner zuschaltet, um den Durchsatz zu erhöhen. Sinkt das Datenaufkommen, wird der zweite ➤➤ **B-Kanal** wieder geschlossen. Bei Aufbau einer Verbindung wird zunächst nur ein B-Kanal geöffnet.

Statisch Bei statischer Kanalbündelung legen Sie von vorneherein fest, ob **BinGO!** einen oder zwei B-Kanäle für Verbindungen zum WAN-Partner nutzen soll, unabhängig von der übertragenen Datenmenge.

Die Konfiguration erfolgt in ***WAN Partner*** ➧ **ADD** ➧ ***Advanced Settings***:

Feld	Bedeutung
Channel-Bundling	Legt fest, ob bzw. welche Art von Kanalbündelung für Verbindungen mit dem WAN-Partner genutzt werden soll.
Total Number of Channels	Bei dynamischer Kanalbündelung: Definiert die maximale Anzahl der B-Kanäle, die geöffnet werden dürfen. Bei statischer Kanalbündelung: Definiert die Anzahl der B-Kanäle, die während der ganzen Verbindung geöffnet sind. Mögliche Werte: *1*, *2*.

Tabelle 7-9: ***WAN Partner*** ➧ ***Edit*** ➧ ***Advanced Settings***

Das Feld *Channel-Bundling* enthält folgende Auswahlmöglichkeiten:

Mögliche Werte	Bedeutung
no	Keine Kanalbündelung, für Verbindungen steht immer nur ein B-Kanal zur Verfügung.
dynamic	Dynamische Kanalbündelung.
static	Statische Kanalbündelung.

Tabelle 7-10: *Channel-Bundling*

ToDo Gehen Sie folgendermaßen vor:

- Gehen Sie zu ***WAN Partner*** ➧ ***Edit*** ➧ ***Advanced Settings***.
- Wählen Sie *Channel-Bundling* aus.
- Geben Sie *Total Number of Channels* ein.
- Bestätigen Sie mit **OK**.
- Bestätigen Sie mit **SAVE**.

7.2.3 Layer 1 Protocol (ISDN-B-Kanal)

ISDN-B-Kanal Sie können das Layer 1 Protocol des ISDN-➤➤ **B-Kanals**, das **BinGO!** für Verbindungen zum WAN-Partner nutzen soll, definieren. Voreingestellt ist das Protokoll für ISDN-Datenverbindungen mit 64 kbps, was der Standard-Wert des B-Kanals ist. Ändern Sie die Einstellung nur, wenn dies ausdrücklich erforderlich ist.

Die Konfiguration erfolgt in ***WAN PARTNER*** ➧ ***EDIT*** ➧ ***ADVANCED SETTINGS***:

Feld	Bedeutung
Layer 1 Protocol	Legt fest, welches Layer 1 Protocol **BinGO!** nutzen soll. Diese Einstellung gilt nur für ausgehende Rufe an den WAN-Partner und für eingehende Rufe vom WAN-Partner, wenn sie anhand der Calling Party's Number identifiziert werden konnten.

Tabelle 7-11: ***WAN PARTNER*** ➧ ***EDIT*** ➧ ***ADVANCED SETTINGS***

Für eingehende Rufe, die nicht anhand der Calling Party's Number identifiziert werden können, verwendet **BinGO!** als Layer 1 Protocol die Einstellungen unter *Item* in ***CM-1BRI, ISDN S0*** ➧ ***INCOMING CALL ANSWERING*** (siehe Kapitel 6.1.4, Seite 133).

Layer 1 Protocol enthält folgende Auswahlmöglichkeiten:

Mögliche Werte	Bedeutung
ISDN 64 kbps	Für ISDN-Datenverbindungen mit 64 kbps. Dies ist der Standart-Wert.
ISDN 56 kbps	Für ISDN-Datenverbindungen mit 56 kbps.
Modem	Auf **BinGO!** nicht verfügbar.
DOVB	Data transmission Over Voice Bearer – nützlich z. B. in den USA, wo Sprachverbindungen manchmal billiger sind als Datenverbindungen.
V.110 (1200 ... 38400)	Für Verbindungen mit V.110 mit Bit-Raten von 1200 bps, 2400 bps,..., 38400 bps.
Modem Profile 1 ... 8	Auf **BinGO!** nicht verfügbar.
PPTP PNS	VPN-Schnittstelle.

Tabelle 7-12: *Layer 1 Protocol*

Die meisten Einträge von *Layer 1 Protocol* entsprechen den Einträgen von *Item* in ***CM-1BRI, ISDN S0*** ➧ ***INCOMING CALL ANSWERING*** (siehe Kapitel 6.1.4, Seite 133).

ToDo Gehen Sie folgendermaßen vor:

- Gehen Sie zu ***WAN PARTNER*** ➧ ***EDIT*** ➧ ***ADVANCED SETTINGS***.
- Wählen Sie *Layer 1 Protocol* aus.
- Bestätigen Sie mit **OK**.
- Bestätigen Sie mit **SAVE**.

7.2.4 IP Transit Network

Wenn Sie einen WAN-Partner auf **BinGO!** eintragen, gibt es verschiedene Möglichkeiten, die IP-Adresse des Partnernetzes anzugeben:

- Sie geben ➤➤ **IP-Adresse** und ➤➤ **Netzmaske** des Partnernetzes an. Dazu müssen Sie diese natürlich kennen.
- Sie verwenden sowohl für **BinGO!** als auch für den WAN-Partner jeweils eine zusätzliche ISDN-IP-Adresse und ISDN-Netzmaske. Damit bauen Sie während der Verbindung ein virtuelles IP-Netzwerk auf, ein sog. Transitnetzwerk. Diese Einstellung benötigen Sie normalerweise nicht, nur bei manchen Spezialkonfigurationen.
- Sie weisen dem WAN-Partner dynamisch für die Dauer der Verbindung eine IP-Adresse aus einem festgelegten IP-Adreß-Pool zu.
- Sie lassen sich vom WAN-Partner dynamisch für die Dauer der Verbindung eine IP-Adresse zuweisen.

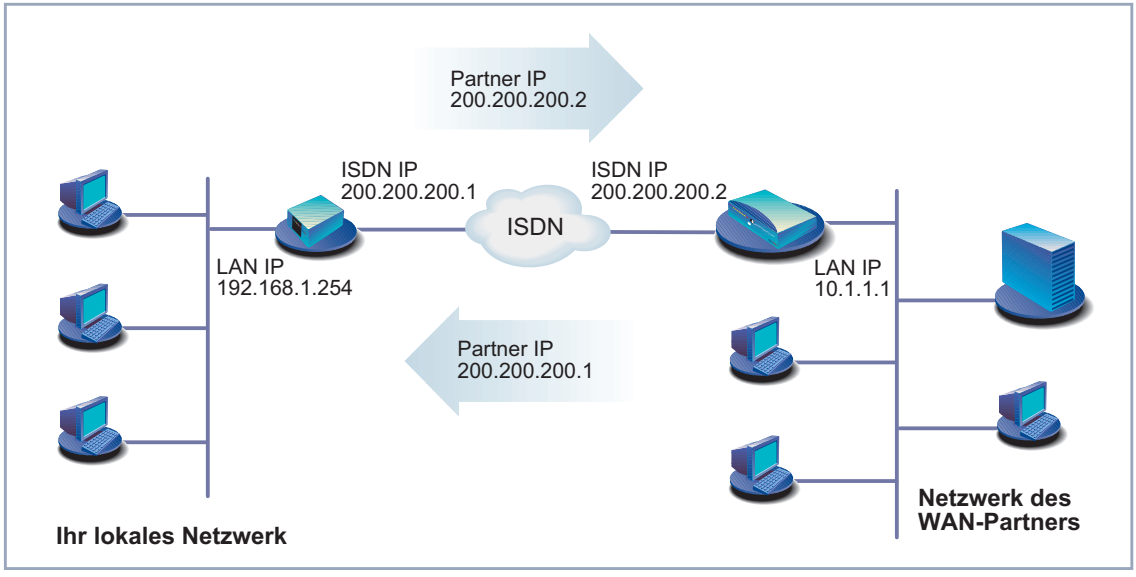


Bild 7-1: LAN-LAN-Kopplung mit Transitnetzwerk

Die Konfiguration erfolgt in ***WAN PARTNER*** ➧ ***EDIT*** ➧ ***IP***:

Feld	Bedeutung
IP Transit Network	Legt fest, ob **BinGO!** ein Transitnetzwerk zum WAN-Partner aufbaut.
local ISDN IP Address	ISDN-IP-Adresse von **BinGO!** im Transitnetzwerk.
Partner's ISDN IP Address	ISDN-IP-Adresse des WAN-Partners im Transitnetzwerk.
Partner's LAN IP Address	IP-Adresse des LAN des WAN-Partners.
Partner's LAN Netmask	Netzmaske des LAN des WAN-Partners. Wenn Sie keinen Eintrag machen, trägt **BinGO!** eine Standard-Netzmaske für die unter *Partner's LAN IP Address* verwendete Netzklasse ein.

Tabelle 7-13: ***WAN PARTNER*** ➧ ***EDIT*** ➧ ***IP***

IP Transit Network enthält folgende Auswahlmöglichkeiten:

Mögliche Werte	Bedeutung
yes	Verwendung eines Transitnetzwerkes.
dynamic client	**BinGO!** erhält seine IP-Adresse für die Dauer der Verbindung vom WAN-Partner.
dynamic server	**BinGO!** weist dem ➤➤ **Remote**-WAN-Partner für die Dauer der Verbindung eine IP-Adresse zu. Dazu muß **BinGO!** als dynamischer IP-Addreß-Server konfiguriert sein, d. h. über einen IP-Adreß-Pool verfügen (siehe Kapitel 7.1.1, Seite 190).
no	Kein Transitnetzwerk. Für die meisten WAN-Partner ist diese Einstellung ausreichend.

Tabelle 7-14: IP Transit Network

ToDo Gehen Sie folgendermaßen vor:

- Gehen Sie zu ***WAN PARTNER*** ➧ ***EDIT*** ➧ ***IP***.
- Wählen Sie *IP Transit Network* aus.
- Geben Sie gegebenenfalls *local ISDN IP Address* ein.
- Geben Sie gegebenenfalls *Partner's ISDN IP Address* ein.
- Geben Sie gegebenenfalls *Partner's LAN IP Address* ein.
- Geben Sie gegebenenfalls *Partner's LAN IP Address* ein.
- Bestätigen Sie mit **SAVE**.

7.2.5 Übermittlung von DNS- und WINS-Server-IP-Adressen an WAN-Partner

IP-Adresse = ? Ein Domain Name Server (➤➤ **DNS**) bzw. Windows Internet Name Server (WINS) wird benötigt, um Host-Namen bzw. ➤➤ **NetBIOS**-Namen in IP-Adressen zu übersetzen (Namensauflösung). Domain Name Server bilden eine

hierarchische Baumstruktur. Sobald eine Anfrage an Ihren primären Domain Name Server gerichtet wird, versucht er, die Namensauflösung mit Hilfe seiner internen Tabellen zu erreichen. Falls er den Namen nicht findet, fragt er bei einem ihm bekannten übergeordneten Domain Name Server nach.

Bei Eintragen eines WAN-Partners auf **BinGO!** können Sie festlegen, ob **BinGO!** Requests nach WINS- bzw. DNS-IP-Adressen sendet oder beantwortet.

Die Konfiguration erfolgt in:

- ***IP*** ➧ ***STATIC SETTINGS***
- ***WAN PARTNER*** ➧ ***EDIT*** ➧ ***IP*** ➧ ***ADVANCED SETTINGS***

Feld	Bedeutung
Primary Domain Name Server	IP-Adresse von **BinGO!**s erstem Domain Name Server (DNS).
Secondary Domain Name Server	IP-Adresse eines weiteren Domain Name Servers.
Primary WINS	IP-Adresse von **BinGO!**s erstem WINS (Windows Internet Name Server) bzw. NBNS (NetBIOS Name Server).
Secondary WINS	IP-Adresse eines weiteren WINS bzw. NBNS.

Tabelle 7-15: ***IP*** ➧ ***STATIC SETTINGS***

Feld	Bedeutung
Dynamic Name Server Negotiation	Legt fest, ob **BinGO!** IP-Adressen für *Primary Domain Name Server*, *Secondary Domain Name Server*, *Primary WINS* und *Secondary WINS* vom WAN-Partner erhält oder an den WAN-Partner sendet.

Tabelle 7-16: ***WAN PARTNER*** ➧ ***EDIT*** ➧ ***IP*** ➧ ***ADVANCED SETTINGS***

Das Feld *Dynamic Name Server Negotiation* enthält folgende Auswahlmöglichkeiten:

Mögliche Werte	Bedeutung
off	**BinGO!** sendet und beantwortet keine Requests nach WINS- bzw. DNS-IP-Adressen.
yes	Das Verhalten ist an den Modus für Vergabe/Empfang einer IP-Adresse gekoppelt (Einstellung in ***WAN PARTNER*** ➧ ***EDIT*** ➧ ***IP*** unter *IP Transit Network*)*:* ■ **BinGO!** sendet Requests nach WINS- bzw. DNS-IP-Adressen an den WAN-Partner, falls *dynamic client* ausgewählt ist. ■ **BinGO!** beantwortet Requests nach WINS- bzw. DNS-IP-Adressen vom WAN-Partner, falls *dynamic server* ausgewählt ist. ■ **BinGO!** sendet und beantwortet keine Requests nach WINS- bzw. DNS-IP-Adressen, falls *yes* oder *no* ausgewählt ist.
client (receive)	**BinGO!** sendet Requests nach WINS- bzw. DNS-IP-Adressen an den WAN-Partner.
server (send)	**BinGO!** beantwortet Requests nach WINS- bzw. DNS-IP-Adressen vom WAN-Partner.

Tabelle 7-17: *Dynamic Name Server Negotiation*

DNS im LAN Falls Sie einen Domain Name Server in Ihrem LAN eingerichtet haben, geben Sie dessen IP-Adresse an.

ToDo Gehen Sie dazu folgendermaßen vor, falls Sie diese Eintragung nicht schon gemacht haben (Kapitel 7.3.2, Seite 222):

➤ Gehen Sie zu ***IP*** ➧ ***STATIC SETTINGS***.

➤ Geben Sie gegebenenfalls *Primary* bzw. *Secondary Domain Name Server* ein.

- Geben Sie gegebenenfalls *Primary* bzw. *Secondary WINS* ein.
- Bestätigen Sie mit **SAVE**.

Gehen Sie folgendermaßen vor, wenn **BinGO!** die eingetragenen Domain Name Server bzw. WINS dem WAN-Partner mitteilen soll (Server-Modus) bzw. wenn bei Verbindungen zum WAN-Partner andere DNS/WINS-Adressen als im LAN verwendet werden sollen (Client-Modus, z. B. bei Einwahl zu einem Internet Service Provider).

- Gehen Sie zu ***WAN PARTNER*** ➧ ***EDIT*** ➧ ***IP*** ➧ ***ADVANCED SETTINGS***.
- Wählen Sie *Dynamic Name Server Negotiation* aus.
- Bestätigen Sie mit **OK**.
- Bestätigen Sie mit **SAVE**.

Wenn Sie keinen Domain Name Server in Ihrem LAN haben (kleinere Netzwerke haben oft keinen eigenen Server), kann die Namensauflösung z. B. über Ihren Internet Service Provider erfolgen (Client-Modus). Dafür sind allerdings ISDN-Verbindungen nötig, die Gebühren kosten.

Wenn Sie mit Windows arbeiten, können Sie eine Namensauflösung auch erreichen, ohne einen DNS zu befragen. Dazu müssen Sie auf allen PCs im LAN die Datei LMHOSTS anpassen. Genaue Informationen dazu in Kapitel 3.6.2, Seite 64.

7.2.6 Routing Information Protocol (RIP)

Routing

Im Allgemeinen kann man Routing so beschreiben: Der ➧➧ **Router** empfängt ➧➧ **Datenpakete**, wobei in jedem Paket der Ziel-Host vermerkt ist. Aufgrund der Eintragungen in der sog. Routing-Tabelle (siehe Kapitel 6.2.1, Seite 152) entscheidet der Router, auf welchem Weg (Route) er das Datenpaket weiterschickt, damit es möglichst schnell (mit möglichst wenigen Zwischenstationen) und günstig ans Ziel gelangt. D. h. der Router propagiert eine Route. Die Eintragungen der Routing-Tabelle können entweder statisch festgelegt werden, oder es erfolgt ein ständiger Update der Routing-Tabelle durch dynamischen Austausch der Routing-Informationen zwischen mehreren Routern. Diesen

Austausch regelt ein sog. Routing-Protokoll, z. B. RIP (Routing Information Protocol).

RIP

Mit ➤➤ **RIP** tauschen Router Ihre in Routing-Tabellen gespeicherten Informationen aus, indem sie in regelmäßigen Abständen miteinander kommunizieren und so gegenseitig Ihre Routing-Einträge ergänzen und erneuern. **BinGO!** unterstützt sowohl Version 1 als auch Version 2 von RIP, entweder exklusiv oder parallel.

RIP wird für LAN und WAN separat konfiguriert.

Aktiv und Passiv

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

WAN-Partner

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

Der Empfang von Routing-Tabellen über RIP ist eventuell ein Sicherheitsloch, da fremde Rechner bzw. Router die Routing-Funktionalität von **BinGO!** verändern können.

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

Die Konfiguration erfolgt in:

- ***WAN Partner*** ➧ ***Edit*** ➧ ***IP*** ➧ ***Advanced Settings***
- ***CM-BNC/TP, Ethernet***

Feld	Bedeutung
RIP Send	Ermöglicht Senden von RIP-Paketen über die Schnittstelle zum WAN-Partner bzw. die LAN-Schnittstelle.
RIP Receive	Ermöglicht Empfangen von RIP-Paketen über die Schnittstelle zum WAN-Partner bzw. die LAN-Schnittstelle.

Tabelle 7-18: ***WAN Partner*** ➧ ***Edit*** ➧ ***IP*** ➧ ***Advanced Settings*** bzw. ***CM-BNC/TP, Ethernet***

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

Mögliche Werte	Bedeutung
none	Nicht aktiviert.
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 7-19: *RIP Send* bzw. *RIP Receive*

ToDo Gehen Sie folgendermaßen vor:

- Gehen Sie zu ***WAN Partner*** ➧ ***Edit*** ➧ ***IP*** ➧ ***Advanced Settings***.
- Wählen Sie *RIP Send* aus.
- Wählen Sie *RIP Receive* aus.
- Bestätigen Sie mit **OK**.
- Bestätigen Sie mit **SAVE**.
- Gehen Sie zu ***CM-BNC/TP, Ethernet***.
- Wählen Sie *RIP Send* aus.
- Wählen Sie *RIP Receive* aus.
- Bestätigen Sie mit **SAVE**.

7.2.7 Komprimierung

Datenkomprimierung Mit Hilfe von ➤➤ **Datenkomprimierung** können Sie den Datendurchsatz erhöhen und damit die Verbindungskosten senken. **BinGO!** unterstützt mehrere

Möglichkeiten, abhängig von der gewählten ➤➤ **Enkapsulierung**, z. B. PPP (siehe Kapitel 6.2.1, Seite 152):

- ➤➤ **STAC**:
  Durch den in **BinGO!** implementierten Industriestandard STAC-Datenkomprimierung (Check Mode 3 in RFC 1974) kann der Durchsatz auf den PPP-ISDN-Verbindungen gesteigert werden.
- MS-STAC:
  STAC-Datenkomprimierung für Windows-➤➤ **Clients** (Check Mode 4 in RFC 1974). Einstellen, wenn man sich bei einem Windows Remote Access Server einwählt.
- ➤➤ **V.42bis**:
  Kompressionsalgorithmus, der eine Sicherungsschicht voraussetzt. Nur möglich bei *Encapsulation = Multi-Protocol LAPB Framing* bzw. *LAPB Framing (only IP)*.
- Van Jacobson Header-Komprimierung (➤➤ **VJHC**):
  Reduziert die Größe von ➤➤ **TCP/IP**-Paketen. Van Jacobson Header-Komprimierung kann zusätzlich zu den obengenannten Kompressionsalgorithmen eingesetzt werden.

Es ist nicht sinnvoll, STAC und V.42bis zusammen für eine Verbindung einzustellen.

Sollte eine Gegenstelle keine Datenkomprimierung unterstützen bzw. die Unterstützung nicht aktiviert haben, so erkennt **BinGO!** dies innerhalb der ➤➤ **PPP**-Verhandlungsphase und deaktiviert die Datenkomprimierung für diese Verbindung.

Die Konfiguration erfolgt in:

- ***WAN PARTNER*** ➧ ***EDIT***
- ***WAN PARTNER*** ➧ ***EDIT*** ➧ ***IP*** ➧ ***ADVANCED SETTINGS***

Feld	Bedeutung
Compression	Legt die Art der Komprimierung für Verbindugen mit dem WAN-Partner fest.

Tabelle 7-20: ***WAN PARTNER*** ➧ ***EDIT***

Das Feld *Compression* enthält folgende Auswahlmöglichkeiten:

Mögliche Werte	Bedeutung
none	Keine Komprimierung.
STAC	Ermöglicht STAC-Datenkomprimierung (wenn *Encapsulation* = *PPP*).
MS-STAC	Ermöglicht STAC-Datenkomprimierung bei Einwahl auf einen Windows Remote Access Server (wenn *Encapsulation* = *PPP*).
MPPC	Auf **BinGO!** nicht verfügbar.
V.42bis	Ermöglicht Datenkomprimierung mit V.42bis (bei *Encapsulation* = *Multi-Protocol LAPB Framing* oder *LAPB Framing (only IP)*).

Tabelle 7-21: *Compression*

Feld	Bedeutung
Van Jacobson Header Compression	Ermöglicht VJHC.

Tabelle 7-22: ***WAN PARTNER*** ➧ ***EDIT*** ➧ ***IP*** ➧ ***ADVANCED SETTINGS***

STAC, MS-STAC, V.42bis

Gehen Sie folgendermaßen vor, um STAC, MS-STAC oder V.42bis einzustellen:

- Gehen Sie zu ***WAN PARTNER*** ➧ ***EDIT*** ➧ ***IP*** ➧ ***ADVANCED SETTINGS***.
- Wählen Sie *Compression* aus.
- Bestätigen Sie mit **SAVE**.

VJHC Gehen Sie folgendermaßen vor, um VJHC einzustellen:

- Gehen Sie zu ***WAN Partner*** ➧ ***Edit*** ➧ ***IP*** ➧ ***Advanced Settings***.
- Aktivieren Sie *Van Jacobson Header Compression: on*.
- Bestätigen Sie mit **OK**.
- Bestätigen Sie mit **SAVE**.

7.2.8 Proxy ARP (Address Resolution Protocol)

ARP-Repuests Mit Hilfe von ➤➤ **Proxy ARP** kann **BinGO!** ➤➤ **ARP**-Requests aus dem LAN beantworten. Wenn ein Host im LAN zu einem anderen Host im LAN oder zu einem WAN-Partner eine Verbindung aufbauen will, aber dessen Hardware-Adresse nicht kennt, sendet er einen sog. ARP-Request als ➤➤ **Broadcast** ins Netz. Er stellt also eine Frage an alle: "Wie lautet die Hardware-Adresse von Host x ?". Wenn auf **BinGO!** Proxy ARP aktiviert ist und der gewünschte Host im LAN oder über eine definierte WAN-Verbindung erreichbar ist, beantwortet **BinGO!** den ARP-Request mit seiner eigenen Adresse. Dies ist für den Verbindungsaufbau ausreichend: Die ➤➤ **Datenpakete** werden an **BinGO!** geschickt, der sie dann an den gewünschten Host weiterleitet. Wenn Proxy ARP nicht aktiviert ist, kann nur der Host mit der geforderten Adresse antworten.

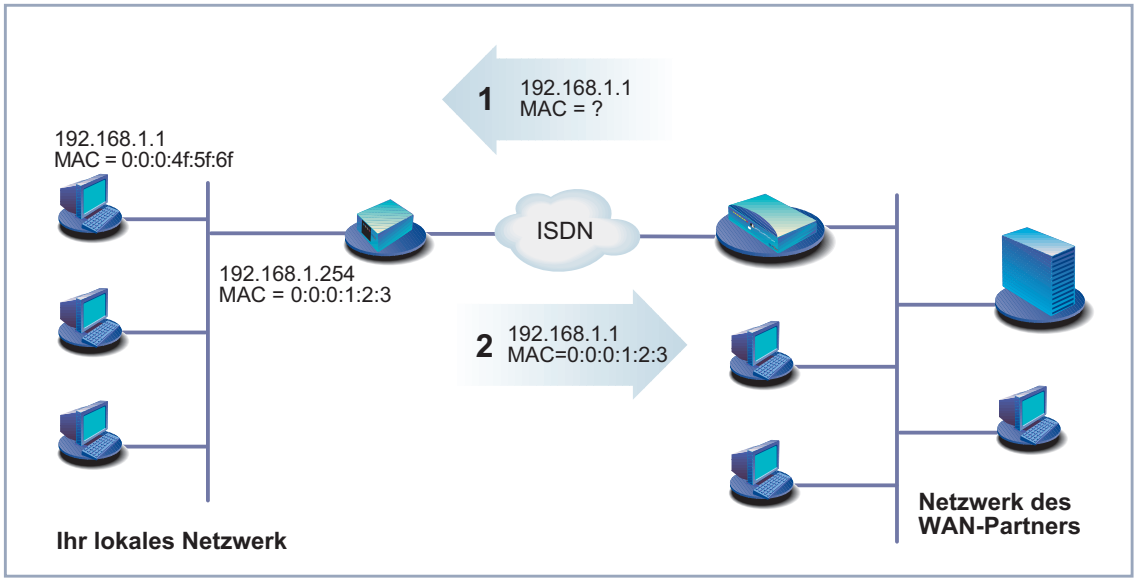


Bild 7-2: Proxy ARP

Beispiel Wenn Rechner im LAN ihre IP-Adressen dynamisch über DHCP zugewiesen bekommen, können für eine Verbindung zu diesen Hosts auf **BinGO!** keine statischen Host-Routen eingetragen werden. Mit Hilfe von Proxy ARP kann trotzdem eine Zuordnung von MAC- und IP-Adressen erfolgen.

Weitere Hinweise (mit Beispiel) zu Proxy ARP finden Sie in der SW-Reference.

Die Konfiguration erfolgt in:

- ***WAN Partner*** ➧ ***Edit*** ➧ ***IP*** ➧ ***Advanced Settings***
- ***CM-BNC/TP, Ethernet***

Feld	Bedeutung
Proxy Arp	Ermöglicht **BinGO!**, ARP-Requests zu beantworten.

Tabelle 7-23: ***WAN Partner*** ➧ ***Edit*** ➧ ***IP*** ➧ ***Advanced Settings*** bzw. ***CM-BNC/TP, Ethernet***

Proxy Arp in ***WAN PARTNER*** ➧ ***EDIT*** ➧ ***IP*** ➧ ***ADVANCED SETTINGS*** enthält folgende Auswahlmöglichkeiten:

Mögliche Werte	Bedeutung
off	Deaktiviert Proxy ARP über die Schnittstelle zum WAN-Partner.
on (up or dormant)	**BinGO!** beantwortet einen ARP-Request nur, wenn der Status der Verbindung zum WAN-Partner *up* (aktiv) oder *dormant* (ruhend) ist. Bei *dormant* beantwortet **BinGO!** lediglich den ARP-Request, der Verbindungsaufbau erfolgt erst, wenn jemand tatsächlich die Route nutzen will.
on (up only)	**BinGO!** beantwortet einen ARP-Request nur, wenn der Status der Verbindung zum WAN-Partner up (aktiv) ist. Damit wird erreicht, daß **BinGO!** einen ARP-Request nur dann beantwortet, wenn bereits eine Verbindung zum WAN-Partner offen ist.

Tabelle 7-24: *Proxy Arp*

Proxy Arp in ***CM-BNC/TP, ETHERNET*** enthält folgende Auswahlmöglichkeiten:

Mögliche Werte	Bedeutung
off	Deaktiviert Proxy ARP über die LAN-Schnittstelle.
on	Ermöglicht Proxy ARP über die LAN-Schnittstelle.

Tabelle 7-25: *Proxy Arp*

ToDo Gehen Sie folgendermaßen vor:

- Gehen Sie zu ***WAN PARTNER*** ➧ ***EDIT*** ➧ ***IP*** ➧ ***ADVANCED SETTINGS***.
- Wählen Sie *Proxy Arp* aus.
- Bestätigen Sie mit **SAVE**.

- Gehen Sie zu ***CM-BNC/TP, ETHERNET***.
- Wählen Sie *Proxy Arp* aus.
- Bestätigen Sie mit **SAVE**.

7.3 Grundlegende IP-Einstellungen

Hier finden Sie einige grundlegende Einstellungen, die Sie auf **BinGO!** festlegen können:

- Beziehen der Systemzeit
- Namensauflösung (➤➤ **DNS**) auf **BinGO!**
- ➤➤ **Port**-Nummern
- ➤➤ **BOOTP** Relay Agent

Im Folgenden werden die jeweils erforderlichen Konfigurationsschritte erläutert.

7.3.1 Systemzeit

Systemzeit Die Systemzeit benötigen Sie, um korrekte Zeitstempel bei der Aufzeichnung von Verbindungsdaten (Accounting) zu erhalten.

Die Konfiguration erfolgt in ***IP*** ➧ ***STATIC SETTINGS***:

Feld	Bedeutung
Time Protocol	Protokoll, das für das Beziehen der aktuellen Zeit benutzt wird. Mögliche Werte: ■ *TIME/UDP* ■ *TIME/TCP* ■ *SNTP* ■ *ISDN* ■ *none*
Time Offset (sec)	Anzahl der Sekunden, die zu der bezogenen Zeit addiert oder subtrahiert wird. Wenn Sie Werte zwischen -24 und +24 eingeben, versteht **BinGO!** die Angabe als Anzahl von Stunden und wandelt sie automatisch in die entsprechende Anzahl von Sekunden um. Beachten Sie: Wenn Sie *isdn* als *Time Protokol* wählen, müssen Sie den *Time Offset* auf *0* setzen. Wenn Sie *Time Offset (sec)* verändern (Zeit zurückstellen), sollte kein Datenfluß bestehen.
Time Update Interval (sec)	Zeitintervall in Sekunden, nach dem die Systemzeit überprüft und evtl. aktualisiert wird. Wenn Sie Werte zwischen 1 und 24 eingeben, versteht **BinGO!** die Angabe als Anzahl von Stunden und wandelt sie automatisch in die entsprechende Anzahl von Sekunden um. Bei *Time Protocol* = *TIME/UDP*, *TIME/TCP* oder *SNTP:* Aktuelle Zeit wird alle *Time Update Interval* Sekunden überprüft. Bei *Time Protocol* = *ISDN:* Aktuelle Zeit wird jeweils bei der ersten ISDN-Verbindung nach Ablauf von *Time Update Interval* überprüft.

Feld	Bedeutung
Time Server	IP-Adresse des Time-➤➤ **Servers**, den **BinGO!** nutzt. *Time Server* wird nicht benötigt, wenn Sie *ISDN* als *Time Protocol* einstellen.

Tabelle 7-26: ***IP*** ➧ ***STATIC SETTINGS***

Das Feld *Time Protocol* enthält folgende Auswahlmöglichkeiten:

Mögliche Werte	Bedeutung
TIME/UDP	Systemzeit (RFC 868) über ➤➤ **UDP**.
TIME/TCP	Systemzeit (RFC 868) über ➤➤ **TCP**.
TIME/SNTP	SNTP (Simple Network Time Protocol, RFC 1769) über UDP.
ISDN	Systemzeit aus ISDN-➤➤ **D-Kanal** (kostenlos).
none	Keine Systemzeit beziehen.

Tabelle 7-27: *Time Protocol*

ISDN Gehen Sie folgendermaßen vor, um die Systemzeit über ISDN zu beziehen:

- ➤ Gehen Sie zu ***IP*** ➧ ***STATIC SETTINGS***.
- ➤ Wählen Sie *Time Protocol* aus: *ISDN*.
- ➤ Geben Sie *Time Offset (sec)* ein: *0*.
- ➤ Geben Sie *Time Update Interval (sec)* ein, z. B. *86400* (entspricht 24 Stunden).
- ➤ Bestätigen Sie mit **SAVE**.

  Nachdem die erste ISDN-Verbindung beendet wurde, bezieht **BinGO!** die Systemzeit über ISDN.

Time-Server Gehen Sie folgendermaßen vor, um die Systemzeit von einem Time-Server zu beziehen:

- ➤ Gehen Sie zu ***IP*** ➧ ***STATIC SETTINGS***.

- Wählen Sie *Time Protocol* aus, z. B. *TIME/UDP*.
- Geben Sie *Time Offset (sec)* ein, z. B. *0*.
- Geben Sie *Time Update Interval (sec)* ein, z. B. *86400* (entspricht 24 Stunden).
- Geben Sie IP-Adresse oder Hostname für *Time Server* ein.
- Bestätigen Sie mit **SAVE**.

  BinGO! bezieht somit die Systemzeit über einen Time-Server. Alle 24 Stunden gleicht **BinGO!** seine Systemzeit mit der am Time-Server eingestellten Zeit ab.

Die ➤➤ **DIME Tools** enthalten einen Time-Server. Wenn Sie die IP-Adresse Ihres PCs bei *Time Server* eintragen, achten Sie darauf, daß bei jedem Start von **BinGO!** die **DIME Tools** auf Ihrem PC aktiv sind.

Wenn Ihr Rechner keine feste IP-Adresse hat, sondern seine IP-Adresse via ➤➤ **DHCP** dynamisch zugewiesen bekommt, können Sie Ihren Rechner nicht als Time-Server verwenden.

7.3.2 Namensauflösung auf BinGO!

Domain Name

Damit **BinGO!** Host-Namen bzw. Computer-Namen im LAN auflösen kann (z. B. für `ping` oder `telnet`), tragen Sie **BinGO!**s Domain Name und die IP-Adresse von DNS- oder WINS-Servern im LAN ein.

Die Konfiguration erfolgt in ***IP*** ➧ ***STATIC SETTINGS***:

Feld	Bedeutung
Domain Name	Legt **BinGO!**s Domain Name fest.
Primary Domain Name Server	IP-Adresse von **BinGO!**s erstem Domain Name Server (DNS).
Secondary Domain Name Server	IP-Adresse eines weiteren Domain Name Servers.
Primary WINS	IP-Adresse von **BinGO!**s erstem WINS (Windows Internet Name Server) bzw. NBNS (NetBIOS Name Server).
Secondary WINS	IP-Adresse eines weiteren WINS bzw. NBNS.

Tabelle 7-28: ***IP*** ➧ ***STATIC SETTINGS***

ToDo Gehen Sie folgendermaßen vor:

- Gehen Sie zu ***IP*** ➧ ***STATIC SETTINGS***.
- Geben Sie *Domain Name* ein, z. B. *bricks.com*.
- Geben Sie gegebenenfalls *Primary* bzw. *Secondary Domain Name Server* ein.
- Geben Sie gegebenenfalls *Primary* bzw. *Secondary WINS* ein.
- Bestätigen Sie mit **SAVE**.

7.3.3 Portnummern

Was ist ein ➤➤ Port? **BinGO!** verfügt über mehrere Dienste bzw. Applikationen, z. B. HTTP, ➤➤ **Telnet**, ➤➤ **FTP**, usw. Um mehrere Dienste auf dem gleichen Host zu erreichen und gewissermaßen ein genaues Ziel für das IP-Paket innerhalb des Hosts anzugeben, gibt man für eine Verbindung zu **BinGO!** neben der IP-Adresse auch einen Port an. So wird die entsprechende Applikation angesprochen. Ports gibt es nur bei den Protokollen TCP und UDP!

BinGO! leitet eingehende ➤➤ **Datenpakete** an den Port mit der zur gewünschten Applikation gehörigen Nummer weiter. Damit wird die entsprechende Applikation von **BinGO!** angesprochen, die eingehenden Daten können verarbeitet werden.

In ***IP*** ➧ ***STATIC SETTINGS*** können Sie einige wichtige Portnummern festlegen:

Normalerweise sind die Einstellungen korrekt. Nehmen Sie hier also nur Änderungen vor, wenn dies nötig ist.

Feld	Bedeutung
Remote CAPI Server TCP port	Port-Nummer für ➤➤ **Remote-CAPI**-Verbindungen: 2662 (festgelegt von IANA, www.iana.com).
Remote TRACE Server TCP port	Port-Nummer für TRACE-Requests. Standardwert: 7000.
RIP UDP port	Port-Nummer für ➤➤ **RIP** (Routing Information Protocol). Standardwert: 520. Mit *RIP UDP port* = *0* kann RIP ausgeschaltet werden.
HTTP TCP port	Port-Nummer für HTTP-Requests. Standardwert: 80. Mit *HTTP TCP port* = *0* wird der Zugriff auf die HTTP-Statusseite von **BinGO!** (siehe Kapitel 8.1.3, Seite 244) verhindert.

Tabelle 7-29: ***IP*** ➧ ***STATIC SETTINGS***

ToDo Gehen Sie folgendermaßen vor, wenn Sie eine der Portnummern verändern wollen:

- ➤ Gehen sie zu ***IP*** ➧ ***STATIC SETTINGS***.
- ➤ Geben Sie *Remote CAPI Server TCP port*, *Remote TRACE Server TCP port*, *RIP UDP port* und/oder *HTTP TCP port* ein.
- ➤ Bestätigen Sie mit **SAVE**.

7.3.4 BOOTP Relay Agent

Bootstrap Protocol

Das Bootstrap Protocol (➤➤ **BOOTP**) definiert, wie ein Host (BOOTP-➤➤ **Client**) in einem TCP/IP-Netzwerk beim Hochfahren seine IP-Adresse und andere Konfigurationsinformationen erhält. Der BOOTP-Client sendet einen BOOTP-Request, ein BOOTP-Server beantwortet den Request mit einem BOOTP-Response und versorgt den Client mit den erforderlichen Informationen. Da der Server nur Requests aus dem LAN, in dem er sich befindet, hört, ist das Einrichten eines BOOTP-Relay-Agent manchmal sinnvoll. Der Agent leitet alle Requests bzw. Responses zwischen Client und Server über eine WAN-Verbindung zu diesem Server weiter.

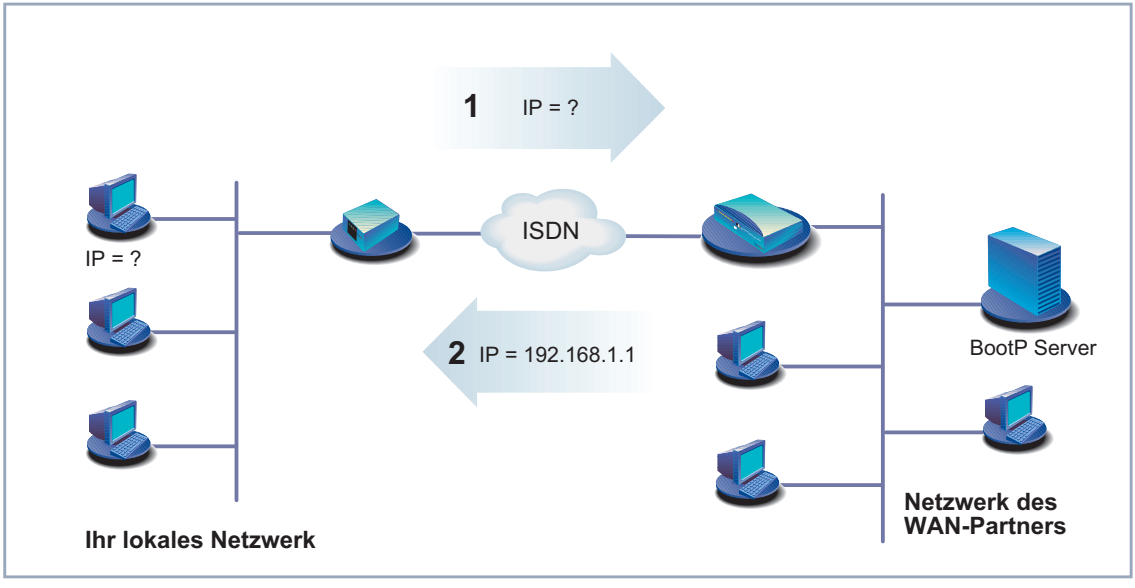


Bild 7-3: **BinGO!** als BOOTP-Relay-Agent

Die Konfiguration erfolgt in ***IP*** ➧ ***STATIC SETTINGS***:

Feld	Bedeutung
BOOTP Relay Server	IP-Adresse des BOOTP-Servers.

Tabelle 7-30: ***IP*** ➧ ***STATIC SETTINGS***

ToDo Gehen Sie folgendermaßen vor:

- Gehen Sie zu ***IP*** ➧ ***STATIC SETTINGS***.
- Geben Sie *BOOTP Relay Server* ein.
- Bestätigen Sie mit **SAVE**.

Wenn für die Verbindung zwischen BOOTP-Server und BOOTP-Client eine ISDN-Verbindung erforderlich ist, muß ein entsprechender WAN-Partner eingerichtet sein (siehe Kapitel 6.2.1, Seite 152).

7.4 IPX-Einstellungen

➤➤ **IPX**-Protokoll (Internet Packet Exchange Protocol) ist ein Netzwerkprotokoll, das hauptsächlich in Novell-Netzwerken verwendet wird. Mit Hilfe von IPX können Novell-➤➤ **Clients** und Novell-➤➤ **Server** über LAN/WAN-Verbindungen kommunizieren.

Im Folgenden werden die Konfigurationsschritte erläutert, die für IPX-Verbindungen erforderlich sind:

- Allgemeine Einstellungen
- LAN-Schnittstelle konfigurieren
- WAN-Partner einrichten

7.4.1 Allgemeine Einstellungen

Hier finden Sie globale Parameter für IPX. Diese Einstellungen sind für alle IPX-Verbindungen von **BinGO!** gültig.

Die Konfiguration erfolgt in ***IPX***:

Feld	Bedeutung
Local System Name	IPX-Systemname von **BinGO!** in Großbuchstaben. Ausrufezeichen, Punkte und Unterstriche sind nicht erlaubt.
Internal Network Number	**BinGO!**s interne Netzwerk-Nummer. Dieser Wert muß unter allen Netzwerk-Nummern im LAN einmalig sein und besteht standardmäßig aus den letzten vier Bytes von **BinGO!**s ➤➤ **MAC-Adresse**. Ändern Sie diesen Wert nur, wenn *Internal Network Number* eines ➤➤ **Remote**-IPX-Router den gleichen Wert hat.
enable IPX spoofing	Aktiviert bzw. deaktiviert NCP session watchdog spoofing und handling of "broadcast message waiting" packets. Mögliche Werte: ■ *yes* ■ *no*
enable SPX spoofing	Aktiviert bzw. deaktiviert spoofing of SPX session watchdog packets. Mögliche Werte: ■ *yes* ■ *no:* using SPX sessions über WAN-Verbindungen wird verhindert.
NetBIOS Broadcast replication	Definiert, wie **BinGO!** mit ➤➤ **NetBIOS**-Paketen verfährt.

Tabelle 7-31: ***IPX***

NetBIOS Broadcast replication enthält folgende Auswahlmöglichkeiten:

Mögliche Werte	Bedeutung
yes	Alle NetBIOS-Hosts im Netzwerk können aufeinander zugreifen, auch wenn häufig WAN-Verbindungen aufgebaut werden müssen.
no	NetBIOS-Hosts in unterschiedlichen LANs haben keinen Zugriff aufeinander.
on LAN only	Nur NetBIOS-Hosts im LAN, für die keine WAN-Verbindungen aufgebaut werden müssen, können aufeinander zugreifen.

Tabelle 7-32: NetBIOS Broadcast replication

ToDo Gehen Sie folgendermaßen vor:

- Gehen Sie zu ***IPX***.
- Geben Sie *Local System Name* ein.
- Geben Sie gegebenenfalls *Internal Network Number* ein (nur wenn nötig!).
- Aktivieren Sie gegebenenfalls *enable IPX spoofing*.
- Aktivieren Sie gegebenenfalls *enable SPX spoofing*.
- Wählen Sie *NetBIOS Broadcast replication* aus.
- Bestätigen Sie mit **SAVE**.

7.4.2 LAN-Schnittstelle konfigurieren

Konfigurieren Sie als nächstes die LAN-Schnittstelle von **BinGO!** zum IPX-Netzwerk. Die LAN-Schnittstelle ist die physikalische Schnittstelle zum lokalen Netzwerk. Im folgenden Menü geben Sie dem Router die Adresse, unter der er im LAN zu erreichen ist. Solange **BinGO!** diese Eintragungen nicht hat, kann er von anderen Hosts nicht als Teil des LANs erkannt werden.

Die Konfiguration erfolgt in ***CM-BNC/TP, ETHERNET***:

Feld	Bedeutung
local IPX-NetNumber	Die IPX-Netzwerk-Nummer des LANs, an das **BinGO!** angeschlossen ist.
Encapsulation	Definiert, welche Art von Header den IPX-Paketen, die über diese LAN-Schnittstelle laufen, hinzugefügt wird. Mögliche Werte: ■ *none* ■ *Ethernet II* ■ *Ethernet 802.2 LLC* ■ *Ethernet SNAP* ■ *Ethernet NOVELL 802.3*

Tabelle 7-33: ***CM-BNC/TP, ETHERNET***

Die zur Verfügung stehenden IPX-➤➤ **Enkapsulierungen** unterstützen z. T. auch IP-Pakete:

IPX-Enkapsulierung	Unterstützte Protokolle	
	IP	IPX
Ethernet II	X	X
Ethernet SNAP	X	X
Ethernet 802.2 LLC		X
Novell 802.3		X

Tabelle 7-34: IPX-Enkapsulierungen

ToDo Gehen Sie folgendermaßen vor:

➤ Gehen Sie zu ***CM-BNC/TP, ETHERNET***.

➤ Geben Sie *local IPX-NetNumber* ein.

- Wählen Sie *Encapsulation* aus.
- Bestätigen Sie mit **SAVE**.

7.4.3 WAN-Partner einrichten

Wenn die Verbindung zu einen oder mehreren WAN-Partnern mit dem IPX-Protokoll realisiert wird, müssen Sie dafür einige Einstellungen festlegen.

Die Konfiguration erfolgt in ***WAN PARTNER*** ➧ ***EDIT*** ➧ ***IPX***:

Feld	Bedeutung
Enable IPX	Ermöglicht IPX für den WAN-Partner. Mögliche Werte: ■ *yes* ■ *no*
IPX NetNumber	IPX-Netzwerknummer der WAN-Verbindung. Wird von einigen IPX-Routern benötigt.
Send RIP/SAP Updates	Definiert, wie oft ➤➤ **RIP**-(Routing Information Protocol) und SAP- (Service Advertising Protocol) Pakete von **BinGO!** zum WAN-Partner geschickt werden. In IPX-Netzwerken werden RIP- und SAP-Pakete als ➤➤ **Broadcasts** in verbundene Netze gesendet, um über aktuelle Routen und Dienste zu informieren und diese auf den neuesten Stand zu bringen. Der dadurch verursachte Datenfluß ist okay im LAN, für über WAN-Verbindungen angeschlossene Netze muß hier eine Einstellung vorgenommen werden.
Update Time	Definiert, in welchen Zeitabständen periodische Updates gesendet werden.
Age Multiplier	Wenn während *Update Time* x *Age Multiplier* eingetragene Routen und Dienste nicht erneuert werden, werden sie gelöscht. Dies verhindert, daß sich unnötig viele Routen und Dienste ansammeln, die nicht genutzt werden.

Tabelle 7-35: ***WAN PARTNER*** ➧ ***EDIT*** ➧ ***IPX***

Das Feld *Send RIP/SAP Updates* enthält folgende Auswahlmöglichkeiten, die mit Hilfe einer Tabelle erläutert werden:

Mögliche Werte	Neue Verbindung wird geöffnet?	Updates?	Periodische Updates?	Beschreibung
off	nie	nein	nein	Alle Routen und Dienste müssen statisch eingetragen werden.
triggered + piggyback (on changes, per. if link active)	nur für Veränderungen	ja	ja	Dies ist die Standard-Einstellung, in den meisten Fällen ausreichend.
triggered (on changes)	nur für Veränderungen	ja	nein	Weniger Datenverkehr als *triggered + piggyback*, aber auch weniger zuverlässig.
piggyback (only if link active)	nie	ja	ja	Mindestens 1 Route bzw. Dienst muß für den WAN-Partner eingetragen werden.
passive triggered (on changes only if link active)	nie	ja	nein	Mindestens 1 Route bzw. Dienst muß für den WAN-Partner eingetragen werden.
time update (always)	immer	ja	ja	Kann zu höheren ISDN-Gebühren führen.

Tabelle 7-36: Send RIP/SAP Updates

ToDo Gehen Sie folgendermaßen vor:

- Wählen Sie *Enable IPX* aus.
- Geben Sie *IPX NetNumber* ein.
- Wählen Sie Send *RIP/SAP Updates* aus.
- Geben Sie gegebenenfalls *Update Time* ein.
- Geben Sie gegebenenfalls *Age Multiplier* ein.
- Bestätigen Sie mit **OK**.
- Bestätigen Sie mit **SAVE**.

7.5 Funktionen mit Zusatzlizenz

In diesem Kapitel wird kurz dargestellt, welche Funktionen Sie auf **BinGO!** mit einer Zusatzlizenz freischalten können.

7.5.1 VPN (Virtual Private Network)

Mit Hilfe von PPTP (Point to Point Tunneling Protocol) kann **BinGO!** ein VPN herstellen. Dies dient zu einer sicheren (verschlüsselten) Übertragung von Daten über WAN-Verbindungen, z. B. über das Internet. So kann von Außendienstmitarbeitern per Laptop ein Zugang auf Daten des Firmennetzes kostengünstig über das Internet realisiert werden (Einwahl über einen örtlichen Internet Service Provider).

Detaillierte Informationen und Konfigurationshinweise (mit Beispielen) finden Sie in Extended Feature Reference.

7.5.2 Unbegrenzte Anzahl LAN-Partner

Mit einer Zusatzlizenz können Sie die Beschränkung auf 8 LAN-Partner in Ihrem Netzwerk aufheben.

8 Sicherheitsmechanismen

SAFERNET

BinTec Communications AG ermöglicht mit **BinGO!** eine hohe Sicherheit Ihres Netzwerks und Ihrer Verbindungen. Die verfügbaren Sicherheits-Funktionen (SAFERNET) erlauben das Überwachen von Aktivitäten über den Router und eine wirksame Zugangs- bzw. Abhörsicherung. Die erforderlichen Konfigurationsschritte werden in diesem Kapitel dargestellt.

Manches können Sie nicht mit Hilfe des Setup Tools konfigurieren, sondern nur durch direktes Eintragen in ➤➤ **MIB**-Tabellen. Die entsprechenden Tabellen bzw. Variablen werden im jeweiligen Abschnitt genannt.

MIB-Einträge können Sie entweder durch Kommandos in der ➤➤ **SNMP-Shell** oder durch externe SNMP-Manager, z. B. DIME Browser, vornehmen. Eine Beschreibung der SNMP-Kommandos finden Sie in der Software Reference.

Das Kapitel ist folgendermaßen aufgebaut:

- Überwachen von Aktivitäten
- Zugangssicherung
- Abhörsicherung
- Besonderheiten
- Checkliste

8.1 Überwachen von Aktivitäten

Eine wesentliche Voraussetzung für einen hohen Grad an Sicherheit ist die Möglichkeit, alle Aktivitäten auf und über den Router hinweg exakt beobachten zu können. Dazu stellt Ihnen BinTec Communications AG eine Vielzahl an Möglichkeiten zur Verfügung.

8.1.1 Syslog-Messages

Alle wesentlichen Ereignisse auf **BinGO!**'s verschiedenen Subsystemen (➤➤ **ISDN**, ➤➤ **PPP**, ➤➤ **CAPI**, usw.) werden in der Form von Syslog-Messages (System logging messages) protokolliert.

Je nach eingestelltem Level (acht Stufen von critical über info bis debug) werden dabei mehr oder weniger viele Details sichtbar. Die protokollierten Daten werden auf **BinGO!** in einer Liste von einstellbarer Länge gespeichert. Alle Informationen können und sollten zur Speicherung und Weiterverarbeitung an einen oder mehrere externe Rechner weitergeleitet werden, z. B. an den Rechner des System-Administrators. Auf **BinGO!** gehen die Syslog-Messages bei einem Neustart verloren.

Vermeiden Sie es, Syslog-Messages auf Log Hosts weiterzuleiten, die über eine Wählverbindung erreicht werden. Dies strapaziert nur unnötig Ihre Telefonrechnung.

Achten Sie darauf, die Syslog-Messages nur an einen sicheren Rechner weiterzuleiten. Kontrollieren Sie die Daten regelmäßig und achten Sie darauf, daß jederzeit ausreichend freie Kapazität auf der Festplatte des Rechners zur Verfügung steht.

Syslog Daemon

Die Erfassung der Syslog-Messages wird von allen Unix-Betriebssystemen unterstützt (Aufsetzen eines Syslog Daemons unter Unix: Siehe Software Reference). Für Windows-Rechner ist in den DIME Tools ein Syslog Daemon enthalten, der die Daten aufzeichnen und je nach Inhalt auf verschiedene Dateien verteilen kann (siehe BRICKware for Windows).

Einstellungen für Syslog-Messages erfolgen in:

- ***SYSTEM***
- ***SYSTEM*** ➧ ***EXTERNAL SYSTEM LOGGING***
- ***WAN PARTNER*** ➧ ***EDIT*** ➧ ***IP*** ➧ ***ADVANCED SETTINGS***

Feld	Bedeutung
Syslog output on serial console	Ermöglicht die Anzeige von Syslog-Messages auf dem mit der seriellen Schnittstelle von **BinGO!** verbundenen Rechner (wenn möglich sollten Sie diese Einstellung vermeiden, da die Verbindung sehr langsam ist). Mögliche Werte: ■ *yes* ■ *no*
Message level for the syslog table	Spezifiziert die Priorität der anzuzeigenden Syslog-Messages. Mögliche Werte: ■ *emerg*: Emergency Messages (höchste Priorität) ■ *alert*: Alert Messages ■ *crit*: Critical Messages ■ *err*: Error Messages ■ *warning*: Warning Messages ■ *notice*: Notice Message ■ *info*: Info Messages ■ *debug*: Debug Messages (niedrigste Priorität) Nur Syslog-Messages mit höherer oder gleicher Priorität wie angegeben werden angezeigt.
Maximum Number of Syslog Entries	Maximale Anzahl an Syslog-Messages, die auf **BinGO!** gespeichert werden.

Tabelle 8-1: ***System***

Feld	Bedeutung
Log Host	➤➤ **IP-Adresse** des Hosts, zu dem Syslog-Messages weitergeleitet werden.
Level	Priorität der zu *Log Host* zu schickenden Syslog-Messages. Entspricht *Message level for the syslog table* in ***SYSTEM***.
Facility	Syslog-Facility auf *Log Host*. Nur erforderlich, wenn der *Log Host* ein Unix-Rechner ist.
Type	Nachrichtentyp. Mögliche Werte: ■ all: Alle Messages. ■ system: Syslog-Messages außer Accounting-Messages. ■ accounting: Accounting-Messages.

Tabelle 8-2: ***SYSTEM*** ➧ ***EXTERNAL SYSTEM LOGGING***

Feld	Bedeutung
IP Accounting	Ermöglicht Speichern von Accounting-Messages für ➤➤ **TCP**-, ➤➤ **UDP**- und ICMP-Sitzungen. Mögliche Werte: *on*, *off*.

Tabelle 8-3: ***WAN PARTNER*** ➧ ***EDIT*** ➧ ***IP*** ➧ ***ADVANCED SETTINGS***

ToDo Gehen Sie folgendermaßen vor, um die gewünschten Einstellungen für Syslog-Messages vorzunehmen:

- ➤ Gehen Sie zu ***SYSTEM***.
- ➤ Wählen Sie *Syslog output on serial console* aus.
- ➤ Wählen Sie *Message level for the syslog table* aus.
- ➤ Geben Sie *Maximum Number of Syslog Entries* ein.

- Gehen Sie zu ***System*** ➧ ***External System Logging***, um Syslog-Messages an externe Hosts weiterzuleiten:
- Wählen Sie einen bestehenden Eintrag aus und bestätigen Sie mit der **Eingabetaste** oder fügen Sie einen neuen Eintrag mit **ADD** hinzu.
- Geben Sie *Log Host* ein.
- Wählen Sie *Level* aus.
- Wählen Sie *Facility* aus.
- Wählen Sie *Type* aus.

Erweitertes IP-Accounting

Gehen Sie folgendermaßen vor, um erweitertes IP-Accounting zu aktivieren. Damit werden auf **BinGO!** Accounting-Messages von TCP-, UDP- und ICMP-Sitzungen gespeichert:

- Gehen Sie zu ***WAN Partner*** ➧ ***Edit*** ➧ ***IP*** ➧ ***Advanced Settings***.
- Aktivieren Sie *IP Accounting* mit *on*.

Anzeige von Syslog-Messages

Gehen Sie folgendermaßen vor, um Syslog-Messages anzuzeigen:

- Gehen Sie zu ***Monitoring and Debugging*** ➧ ***Messages***.

  Hier werden die auf **BinGO!** gespeicherten Syslog-Messages angezeigt:

```
BinGO! Setup Tool                              BinTec Communications AG
[MONITOR][MESSAGE]: Syslog Messages                             MyBinGO!

Subj    Lev Message

SNMP    DEB sent TRAP (linkUp,0) 115 bytes to circindex 1001 Port 36880
SNMP    DEB sent TRAP (linkUp,0) 115 bytes to 199.1.1.13 Port 162




Press <Ctrl-n>, <Ctrl-p> to scroll
```

Löschen von Syslog-Messages

- Wählen Sie **RESET**, um die Syslog-Messages auf **BinGO!** zu löschen.

Zur Interpretation von Syslog-Messages: Siehe Software Reference.

8.1.2 Monitorfunktionen im Setup Tool

Neben Syslog-Messages können Sie mit Hilfe des Setup Tools noch einige weitere Daten anzeigen. Dabei wird jeweils durch periodische Aktualisierung der aktuelle Status von bestimmten Teilsystemen dargestellt. Zu den folgenden Funktionsbereichen existieren Anzeigenmodule:

- ISDN-Verbindungen
- Taschengeldkonto
- Schnittstellen-Statistik (vergleichende Darstellung mehrerer Schnittstellen)
- ➤➤ **TCP/IP**-Statistik
- Syslog-Messages (siehe Kap. Kapitel 8.1.1, Seite 236)

ISDN-Verbindungen

Gehen Sie folgendermaßen vor, um ISDN-Verbindungen anzuzeigen:

➤ Gehen Sie zu ***MONITORING AND DEBUGGING*** ➧ ***ISDN MONITOR***.

Eine Liste der bestehenden ISDN-Verbindungen (eingehend und ausgehend) wird angezeigt.

```
BinGO! Setup Tool                              BinTec Communications AG
[MONITOR][ISDN CALLS]: ISDN Monitor - Calls                    MyBinGO!

Dir Remote Name/Number   Charge  DurationeStack   Channel  State

in  2                            2910        0       B1       active
out 3                            106         0       B2
disc_req


(c)alls        (h)istory        (d)etails        (s)tatistics
(r)elease
```

Weitere Optionen stehen Ihnen in diesem Menü zur Verfügung:

➤ Wählen Sie **h**, um eine Liste der letzten 20 seit dem letzten Systemstart abgeschlossenen ISDN-Verbindungen (eingehend und ausgehend) anzuzeigen.

➤ Setzen Sie den Cursor auf eine bestehende oder abgeschlossene ISDN-Verbindung und wählen Sie **d**, um detaillierte Informationen darüber anzuzeigen.

- Wählen Sie **s**, um eine Statistik über die Aktivität der bestehenden ISDN-Verbindungen anzuzeigen.
- Wählen Sie **c**, um wieder die Liste der bestehenden ISDN-Verbindungen anzuzeigen.
- Wählen Sie **r**, um die mit der **Leertaste** markierte ISDN-Verbindung zu schließen.

Taschengeldkonto

Gehen Sie folgendermaßen vor, um den Stand des Taschengeldkontos anzuzeigen:

- Gehen Sie zu ***MONITORING AND DEBUGGING*** ➧ ***ISDN CREDITS***.
- Wählen Sie ein Subsystem aus und bestätigen Sie mit der **Eingabetaste**.

  Der aktuelle Stand des Taschengeldkontos für das ausgewählte Subsystem wird angezeigt.

```
BinGO! Setup Tool                              BinTec Communications AG
[MONITOR][CREDITS][STAT]: Monitor isdnlogin Credits           MyBinGO!


                                      Total    Maximum      % reached
Time till end of measure interval (sec)7794   86400        91

Number of Incoming Connections               0          2   0
Number of Outgoing Connections               0        20    0

Time of Incoming Connections                    428800     0
Time of Outgoing Connections                   1328800     0

Charge                                       0

EXIT
```

Schnittstellen-Statistik

Gehen Sie folgendermaßen vor, um aktuelle Werte und Aktivitäten der **BinGO!**-Schnittstellen anzuzeigen:

- Gehen Sie zu ***MONITORING AND DEBUGGING*** ➧ ***INTERFACES***.

  Die Werte von zwei Schnittstellen werden nebeneinander angezeigt.

```
BinGO! Setup Tool                                BinTec Communications AG
[MONITOR][INTERFACE]: Interface Monitoring                       MyBinGO!

Interface Name       en1                         PROVIDER
Operational Status   up                          dormant

                     total    per second         total    per second

Received Packets     5512     0                  0        0
Received Octets      920664   0                  0        0
Received Errors      0                           0

Transmit Packets     9        0                  0        0
Transmit Octets      1193     0                  0        0
Transmit Errors      0                           0

Active Connections   N/A                         0
Duration             N/A                         0

EXIT                 EXTENDED                    EXTENDED

Use <Space> to select
```

- Wählen Sie unter *Interface Name* die anzuzeigende Schnittstelle aus.
- Wählen Sie **EXTENDED**, um zusätzliche Informationen anzuzeigen. Anschließend können Sie unter *Operation* den Status der Schnittstelle verändern und die Eingabe mit **START OPERATION** bestätigen.

TCP/IP-Statistik

Gehen Sie folgendermaßen vor, um eine Statistik der Verbindungen mit den ➤➤ **Protokollen** ICMP, ➤➤ **IP**, UDP und TCP anzuzeigen:

- Gehen Sie zu ***MONITORING AND DEBUGGING*** ➧ ***TCP/IP***.

  Die Statistik für IP-Verbindungen wird angezeigt. Die Bedeutung der MIB-Variablen finden Sie in der MIB Reference.

```
BinGO! Setup Tool                                BinTec Communications AG
[MONITOR][IP]: IP Statistics                                      MyBinGO!


InReceives           3912        OutNoRoutes          0
InHdrErrors          0           ReasmTimeout         500
InAddrErrors         0           ReasmReqds           0
ForwDatagrams        0           ReasmOKs             0
InUnknownProtos      0           ReasmFails           0
InDiscards           0           FragOKs              0
InDelivers           3321        FragFails            0
OutRequests          9           FragCreates          0
OutDiscards          0           RoutingDiscards      0

EXIT

         I(C)MP              (I)P              (U)DP              (T)CP
```

- Wählen Sie **c**, um eine Verbindungsstatistik von ICMP darzustellen.
- Wählen Sie **i**, um eine Verbindungsstatistik von IP darzustellen.
- Wählen Sie **u**, um eine Verbindungsstatistik von UDP darzustellen.
- Wählen Sie **t**, um eine Verbindungsstatistik von ICMP darzustellen.

8.1.3 HTTP-Statusseite

Jeder BinTec-Router verfügt über eine Homepage, die sog. HTTP-Statusseite. Damit können Sie mit Hilfe eines Internet Browsers (z. B. Netscape Navigator, Internet Explorer) den Status von **BinGO!** anzeigen. So können alle Benutzer des **BinGO!**-LANs, sofern Sie das Paßwort des Benutzernamens `http` kennen, Einblick in den Status des Routers nehmen.

Bitte beachten Sie: HTTP-Seiten werden meist im Cache-Speicher des Browsers gehalten, so daß sie evtl. durch andere Benutzer am selben Arbeitsplatz gelesen werden können und evtl. auch auf beteiligten Proxy-➤➤ **Servern** sichtbar sind.

- Geben Sie die URL `http://<System Name>` in Ihren Browser ein.

  Die HTTP-Statusseite des BinTec-Routers mit dem Systemnamen <System Name> wird angezeigt.

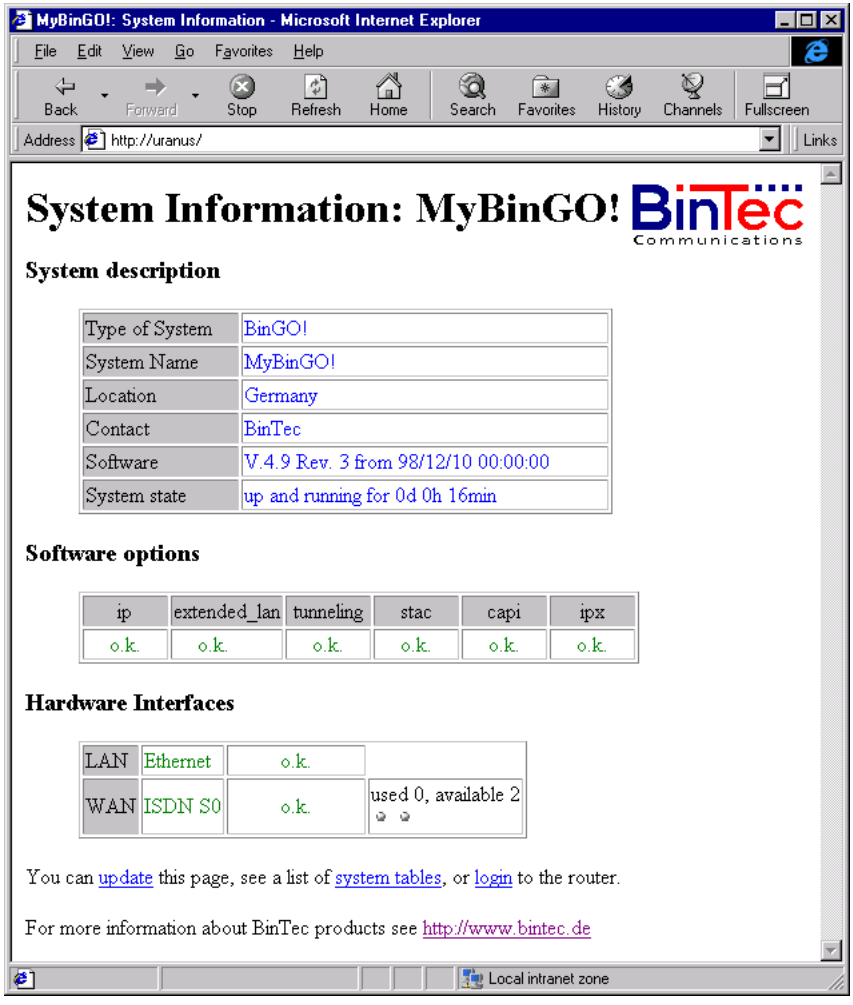


Bild 8-1: HTTP-Statusseite

Die HTTP-Statusseite enthält drei Tabellen:

- System description:
  Hier sind Informationen aus der MIB-Tabelle **admin** aufgelistet, wie **System Name** und **Contact**. Wenn unter **Contact** eine gültige E-Mail-Adresse angegeben ist, ist diese unterstrichen dargestellt.
- Software options:
  Hier sind Informationen aus der MIB-Tabelle **biboAdmLicInfoTable** aufgelistet, der Status von **BinGO!**'s Subsystemen wird angezeigt.
- Hardware Interfaces:
  Hier werden die LAN- und WAN-Schnittstelle von **BinGO!** angezeigt. Die dritte Spalte der Tabelle informiert über den aktuellen Status der physikalischen Schnittstellen mit folgenden möglichen Werten:

Schnittstelle	Status	Mögliche Ursache
LAN	o.k.	Normaler Betrieb.
	inactive	LAN-Kabel ist nicht angeschlossen.
WAN	o.k.	Normaler Betrieb.
	inactive	Keiner der B-Kanäle wird im Moment genutzt.
	unconfigured	ISDN-Kabel ist nicht angeschlossen oder ein falsches ➤➤ **D-Kanal**-Protokoll ist eingetragen.

Tabelle 8-4: Status der Schnittstellen

Die HTTP-Statusseite enthält einige Links:

- update
  Klicken Sie update, um die Statusseite zu aktualisieren.
- login
  Klicken Sie login, um sich auf den dazugehörigen BinTec-Router via ➤➤ **telnet** einzuloggen.

- http://www.bintec.de
  Damit gelangen Sie auf BinTec's WWW-Server mit den neuesten Informationen zu den Produkten und aktueller System-Software und Dokumentation für **BinGO!**.
- system tables
  Klicken Sie auf system tables, um eine Liste mit allen MIB-Tabellen von **BinGO!** anzuzeigen. Durch Anklicken eines Tabellen-Namen werden die darin enthaltenen Variablen aufgelistet.

Wenn Sie die Anzeige von **BinGO!**'s HTTP-Statusseite verhindern möchten, dann tragen Sie als Portnummer des http-Ports 0 ein:

➤ Gehen Sie zu ***IP*** ➧ ***STATIC SETTINGS***.

➤ Geben Sie *HTTP TCP port* ein: *0*.

➤ Bestätigen Sie mit **SAVE**.

8.1.4 JAVA Statusmonitor

Mit dem Java Statusmonitor steht Ihnen eine weitere Möglichkeit zur Verfügung, mit einem Internet-Browser Informationen über **BinGO!** darzustellen. Folgende Daten sind damit abrufbar:

- Statische Informationen wie Systemname des BinTec-Routers und Software-Version
- Datenfluß über die einzelnen Schnittstellen
- Verbindungen zu WAN-Partnern

Wenn Sie den JAVA Statusmonitor zusammen mit der BRICKware installiert haben (siehe Kapitel 3.3, Seite 46), können Sie ihn folgendermaßen starten:

➤ Klicken Sie im Windows-Startmenü auf **Program** ➧ **BRICKware** ➧ **Java Status Monitor**.

Der JAVA Statusmonitor öffnet sich mit Ihrem Standard-Browser.

Weitere Erklärungen zum JAVA Statusmonitor finden Sie in BRICKware for Windows.

8.2 Zugangssicherung

Es gibt einige Möglichkeiten, das Einloggen und Zugreifen auf **BinGO!** nur autorisierten Benutzern zu ermöglichen.

8.2.1 Einloggen

Paßwort

Das Einloggen auf **BinGO!** kann wie in Kapitel 5, Seite 101 beschrieben über mehrere Wege erfolgen, ist aber immer paßwortgesichert. Jeder Fehlversuch wird mit Angabe der Quelle per Syslog-Message protokolliert und erzeugt einen entsprechenden SNMP-Trap. Nach mehreren Fehlversuchen werden Pausen eingeführt, um ein automatisiertes Ausprobieren zu erschweren.

Achtung!

Alle BinTec-Router werden mit gleichen Benutzernamen und Paßwörtern ausgeliefert. Sie sind daher nicht gegen einen unauthorisierten Zugriff geschützt, solange die Paßwörter nicht geändert wurden.

- Ändern sie unbedingt die Paßwörter wie in Kapitel 6.1.2, Seite 128 beschrieben.
- Achten Sie zusätzlich darauf, daß Unbefugte nicht auf die Stromzufuhr zu **BinGO!**, die serielle Konsole und den ➤➤ **Ethernet**-Anschluß zugreifen können.

Solange das voreingestellte Standard-Paßwort für den Benutzernamen `admin` nicht geändert wurde, wird nach dem Einloggen immer eine Warnung ausgegeben.

Autologout

Um unberechtigte Zugriffe zu erschweren, wird die Verbindung zu **BinGO!** getrennt, wenn 15 Minuten lang keine Eingabe über die Tastatur erfolgt. Den Zeitraum können Sie mit dem Kommando `t <Zeit in Sekunden>` verändern (siehe Kapitel 12.1, Seite 316).

Wenn Sie ein Software-Update durchführen (siehe Kapitel 9.2, Seite 288), sollten Sie den Autologout ausschalten: Geben Sie `t 0` in die SNMP-Shell ein.

Es ist möglich, zusätzliche Benutzeraccounts mit Hilfe von SNMP-Kommandos anzulegen (siehe Software Reference). Einem Benutzer kann dabei ein bestimmtes Paßwort und eine bestimmte Aktion zugeordnet werden.

8.2.2 Überprüfen der eingehenden Rufnummer

CLID

Mit Hilfe von Calling Line Identification (➤➤ **CLID**) überprüft **BinGO!** die Calling Party's Number eines eingehenden Rufes.

Screening-Indikator

Darüberhinaus können Sie feststellen, ob eingehende Rufnummern vom Anrufer modifiziert wurden. Bei manchen Anschlüssen ist es möglich, daß statt der eigenen Rufnummer (z. B. 1234) eine andere Nummer (z. B. 5678) beim Angerufenen angezeigt wird. Dies kann **BinGO!** anhand des Screening-Indikators in der Setup-Nachricht des ISDN-➤➤ **D-Kanals** erkennen. Für den Screening-Indikator gibt es vier Werte:

- *user*: Die Angabe der Calling Party's Number stammt von der Gegenseite und wurde vom Netz nicht überprüft.
- *user_verified*: Die Calling Party's Number wurde von der Vermittlungsstelle geprüft und ist richtig.
- *user_failed*: Die Calling Party's Number wurde von der Vermittlungsstelle geprüft und ist falsch.
- *network*: Die Angabe der Calling Party's Number stammt direkt von der Vermittlungsstelle (Normalfall).

Wenn **BinGO!** bei eingehenden Rufen den Screen-Indikator überprüfen soll, müssen Sie einen der genannten Werte in den folgenden MIB-Tabellen bzw. MIB-Variablen eintragen (nur eingehende Rufe mit dem passenden Screening-Indikator werden angenommen):

- Für eingehende PPP-Verbindungen: Variable **Screening** in der Tabelle **biboDialTable**.
- Für eingehende ISDN-Login-Verbindungen: Variable **Screening** in der Tabelle **isdnloginAllowTable**.

8.2.3 Authentisierung von PPP-Verbindungen mit PAP, CHAP oder MS-CHAP

➤➤ **PAP**, ➤➤ **CHAP** und MS-CHAP sind die gebräuchlichen Verfahren zur Authentisierung von ➤➤ **PPP**-Verbindungen. Dabei werden durch ein standardisiertes Verfahren eine Benutzer-ID und ein Paßwort zur Überprüfung der Identität der Gegenstelle ausgetauscht. Weitere Informationen finden Sie in Kapitel 6.2.1, Seite 152 und Kapitel 7.1.4, Seite 198.

8.2.4 Callback

Rückruf

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. **BinGO!** kann sowohl einen eingehenden Ruf mit einem Rückruf beantworten, also auch sich bei einem WAN-Partner einwählen und dann einen Rückruf erwarten:

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

Weitere Informationen zum Callback-Mechanismus finden Sie in der Software Reference.

Die Konfiguration erfolgt in ***WAN Partner*** ➧ ***Edit*** ➧ ***Advanced Settings***:

Feld	Bedeutung
Callback	Aktiviert die Funktion Callback.

Tabelle 8-5: ***WAN Partner*** ➧ ***Edit*** ➧ ***Advanced Settings***

Callback enthält folgende Auswahlmöglichkeiten:

Mögliche Werte	Bedeutung
no	**BinGO!** führt keinen Rückruf aus.
expected (awaiting call-back)	**BinGO!** ruft den WAN-Partner an, um den Call-back zu initiieren.
yes (PPP negotiation)	**BinGO!** ruft zurück mit der Rufnummer, die für den WAN-Partner eingetragen ist. Wenn keine Nummer eingetragen ist, kann die erforderliche Nummer vom Anrufer in einer PPP-Verhandlung mitgeteilt werden. Diese Einstellung ist aus Sicherheitsgründen möglichst zu vermeiden. Bei der Anbindung von Microsoft-➤➤ **Clients** über DFÜ-Netzwerk ist derzeit aber keine Alternative verfügbar.
yes (delayed)	**BinGO!** ruft nach ca. vier Sekunden zurück, wenn Ihr Router vom WAN-Partner dazu aufgefordert wird.
yes	**BinGO!** ruft sofort zurück, wenn Ihr Router vom WAN-Partner dazu aufgefordert wird.

Tabelle 8-6: *Callback*

ToDo Gehen Sie folgendermaßen vor, um Callback für einen WAN-Partner zu aktivieren:

- Gehen Sie zu ***WAN Partner*** ➧ ***Edit*** ➧ ***Advanced Settings***.
- Wählen Sie *Callback* aus.
- Bestätigen Sie mit **OK**.

8.2.5 Closed User Group

BinGO! unterstützt die Nutzung des Dienstmerkmals Geschlosse Benutzergruppe, das Sie bei Ihrer Telefongesellschaft für Ihren ISDN-Anschluß beantra-

gen können. Damit wird die externe/interne Erreichbarkeit durch die Vermittlungsstellen überwacht und geregelt.

ToDo Gehen Sie folgendermaßen vor, um eine Geschlossene Benutzergruppe für einen WAN-Partner zu aktivieren:

- Gehen Sie zu ***WAN Partner*** ➧ ***Edit*** ➧ ***WAN Numbers*** ➧ ***Edit*** ➧ ***Advanced Settings***.
- Wählen Sie *Closed User Group* aus: *specify*.
- Geben Sie den den CUG-Index ein.
- Bestätigen Sie mit **OK**.

8.2.6 Zugriff auf Remote-CAPI

Zu den Besonderheiten der BinTec-Router gehört die Implementierung der Programmierschnittstellen ➤➤ **Remote-CAPI** und Remote-TAPI (nur bei PABX-Geräten). Dadurch können Applikationen auf Rechnern im LAN die Resourcen des Routers nutzen, so als wären diese Komponenten direkt im Rechner eingebaut.

CAPI User Concept Durch Nutzung von BinTec's ➤➤ **CAPI** User Concept können Sie sicherstellen, daß nur durch Benutzername und Paßwort authentisierte Benutzer auf die Remote-CAPI-Schnittstelle von **BinGO!** zugreifen können (siehe Kapitel 7.1.2, Seite 192).

Filter Mit der Definition von Filtern (siehe Kapitel 8.2.8, Seite 258) und lokalen Filtern (siehe Kapitel 8.2.9, Seite 270) können Sie unbefugten Zugriff ebenfalls verhindern.

8.2.7 NAT (Network Address Translation)

➤➤ **NAT** ist ein einfach zu bedienendes Verfahren, das in der Implementierung von BinTec zu vier Zwecken benutzt werden kann:

- Verbergen der internen Host-Adressen eines LANs durch Ummappen auf eine oder mehrere externe Adressen. Die externen Adressen bleiben dabei unverändert.

- Regelung des Zugangs von extern nach intern. Nach extern leitet der Router alle ➤➤ **Datenpakete** weiter, nach intern leitet er nur weiter, was auch explizit freigegeben wurde (Forward NAT).

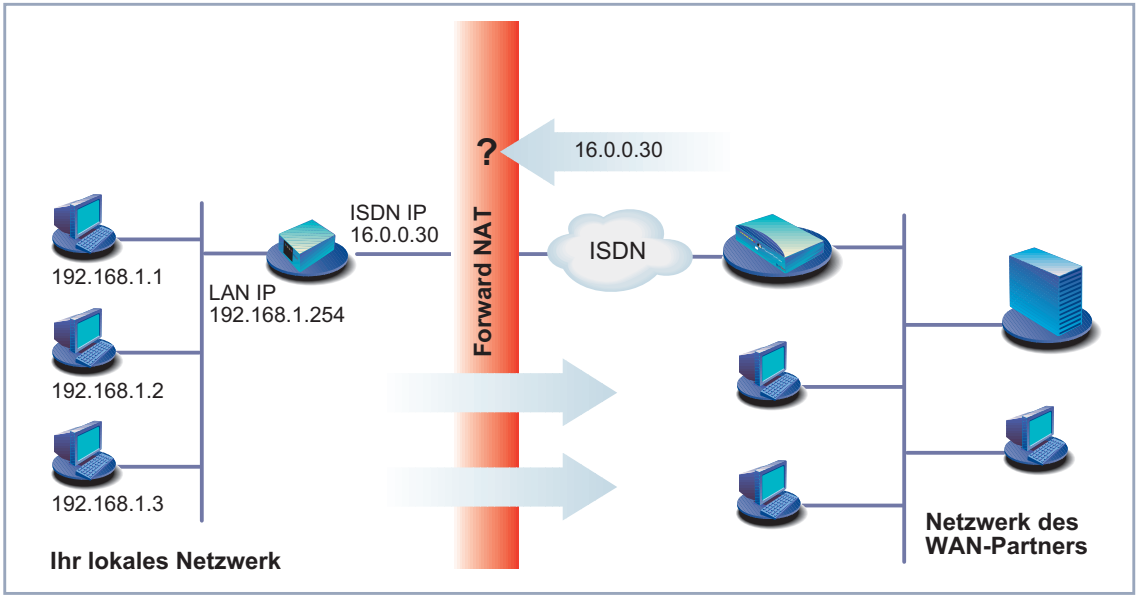


Bild 8-2: Forward NAT

- Mit Reverse NAT wird sichergestellt, daß ein Verbindungspartner nur eine einzige ➤➤ **IP-Adresse** verwendet. Nur eingehende Verbindungen von diesem Partner sind erlaubt, z. B. als Dienstleistung von Internet Service Providern (ISP).

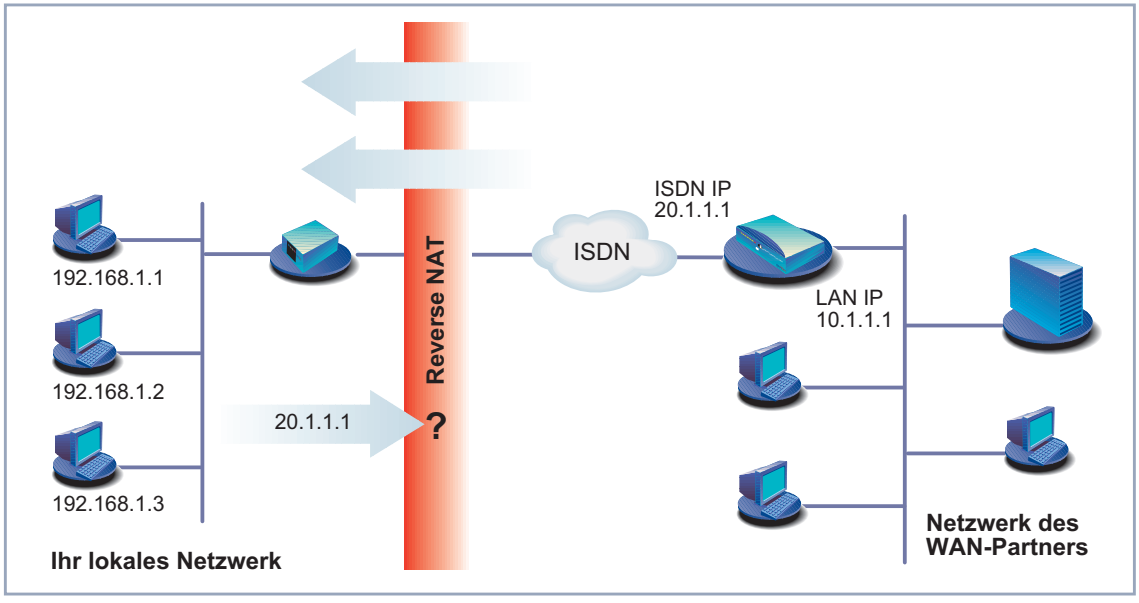


Bild 8-3: Reverse NAT

- Permanente Überwachung der Verbindungen in bzw. aus einem Netzwerk über den Router mit Quell- und Zielangabe der Adressen und ➤➤ **Ports**.

NAT bezieht sich immer auf eine Schnittstelle. **BinGO!**s LAN-Seite wird dabei immer als "innen" bezeichnet, der WAN-Partner befindet sich "außen".

Weitere Erklärungen zu NAT finden Sie in der Software Reference.

Die Konfiguration erfolgt in ***IP*** ➧ ***NETWORK ADDRESS TRANSLATION***.

In ***IP*** ➧ ***NETWORK ADDRESS TRANSLATION*** ➧ **Eingabetaste** aktivieren Sie NAT für eine Schnittstelle von **BinGO!**:

Feld	Bedeutung
Network Address Translation	Definiert die Art von NAT für die ausgewählte Schnittstelle. Mögliche Werte: ■ *off:* Kein NAT ausführen. ■ *on:* Forward NAT ausführen. ■ *reverse:* Reverse NAT ausführen.

Tabelle 8-7: ***IP*** ➧ ***NETWORK ADDRESS TRANSLATION*** ➧ **Eingabetaste**

In ***IP*** ➧ ***NETWORK ADDRESS TRANSLATION*** ➧ **Eingabetaste** ➧ **ADD** können Sie für eine NAT-Schnittstelle bestimmte IP-Verbindungen an einen bestimmten internen Host explizit erlauben:

Feld	Bedeutung
Service	Dienst, der für Verbindungen des unter *Destination* definierten Hosts erlaubt wird. Mögliche Werte: ■ *ftp* ■ *telnet* ■ *smtp* ■ *domain/udp* ■ *domain/tcp* ■ *http* ■ *nntp* ■ *user defined:* Wenn Sie keinen der vordefinierten Dienste verwenden. Geben Sie unter *Protocol* und *Port* die erforderlichen Werte ein, um einen Dienst zu definieren.
Protocol	Nur bei *Service* = *user defined*. Definiert das erlaubte Protokoll. Mögliche Werte: ■ *icmp* ■ *tcp* ■ *udp*
Port (-1 for any)	Nur bei *Service* = *user defined*. Definiert den erlaubten Port. Mit -1 erlauben Sie für Protocol alle Ports. Wenn Sie den Port spezifizieren, muß die Eingabe mit der internen Port-Nummer von **BinGO!** übereinstimmen.

Feld	Bedeutung
Destination	IP-Adresse des Hosts im LAN. Wenn Sie hier keinen Eintrag machen, wird **BinGO!** als Destination angenommen.

Tabelle 8-8: ***IP*** ➧ ***NETWORK ADDRESS TRANSLATION*** ➧ **Eingabetaste** ➧ **ADD**

ToDo Gehen Sie folgendermaßen vor, um NAT zu aktivieren:

- Gehen Sie zu ***IP*** ➧ ***NETWORK ADDRESS TRANSLATION***.
- Wählen Sie die Schnittstelle, für die Sie NAT aktivieren wollen, aus und bestätigen Sie mit der **Eingabetaste**.
- Wählen Sie *Network Address Translation* aus, z. B. *on*.

  Damit ist NAT für die Schnittstelle aktivert.
- Bestätigen Sie mit **SAVE**.

Sobald Sie hier einen Eintrag mit **SAVE** bestätigen, wird dieser sofort wirksam. Denken Sie immer daran, insbesondere wenn Sie NAT von einem Remote-Host konfigurieren, z. B. mit telnet!

Gehen Sie folgendermaßen vor, um für eine NAT-Schnittstelle bestimmte Verbindungen an einen bestimmten Host im LAN freizugeben:

- Gehen Sie zu ***IP*** ➧ ***NETWORK ADDRESS TRANSLATION*** ➧ **Eingabetaste**.
- Fügen Sie mit **ADD** einen Eintrag hinzu oder wählen Sie einen bestehenden Eintrag aus und bestätigen Sie mit der **Eingabetaste**.
- Wählen Sie *Service* aus.
- Wählen Sie gegebenenfalls *Protocol* aus.
- Geben Sie gegebenenfalls *Port (-1 for any)* ein.
- Geben Sie *Destination* ein.
- Bestätigen Sie mit **SAVE**.
- Wiederholen Sie diese Schritte, um mehrere Session Profiles für die ausgewählte NAT-Schnittstelle zu definieren.

8.2.8 Filter

➤➤ **Filter** auf **BinGO!** basieren auf einem Konzept von Filtern, Regeln und sogenannten Ketten. Filter reagieren auf eingehende Datenpakete, sie können also bestimmten Daten das Überqueren von **BinGO!** erlauben oder verbieten.

Filter Ein Filter beschreibt einen Teil des IP-Datenverkehrs, basierend auf IP-Adresse, ➤➤ **Netzmaske**, Protokoll, Quell- und/oder Zielport. Wenn Sie also ein Filter definieren, teilen Sie **BinGO!** mit: "Achte auf alle eingehenden Datenpakete, auf die Folgendes zutrifft: ...".

Regel Mit einer Regel teilen Sie **BinGO!** mit, wie er mit den ausgefilterten Datenpaketen umgehen soll – ob er sie durchlassen oder abweisen soll. Sie können auch mehrere Regeln definieren, die Sie in Form einer Kette organisieren und ihnen damit eine bestimmte Reihenfolge geben.

Kette Im Prinzip gibt es für die Definition von Regeln bzw. Regelketten zwei Möglichkeiten:

- Erlaube alle Pakete, die nicht explizit verboten sind, d. h.:
  - Weise alle Pakete ab, auf die Filter 1 zutrifft.
  - Weise alle Pakete ab, auf die Filter 2 zutrifft.
  - ...
  - ...
  - Laß den Rest durch.
- Laß nur durch, was explizit erlaubt ist, d. h.:
  - Laß alle Pakete durch, auf die Filter 1 zutrifft.
  - Laß alle Pakete durch, auf die Filter 2 zutrifft.
  - ...
  - ...

Schnittstelle Schließlich können Sie noch die Reihenfolge der Regeln für jede **BinGO!**-Schnittstelle individuell festlegen.

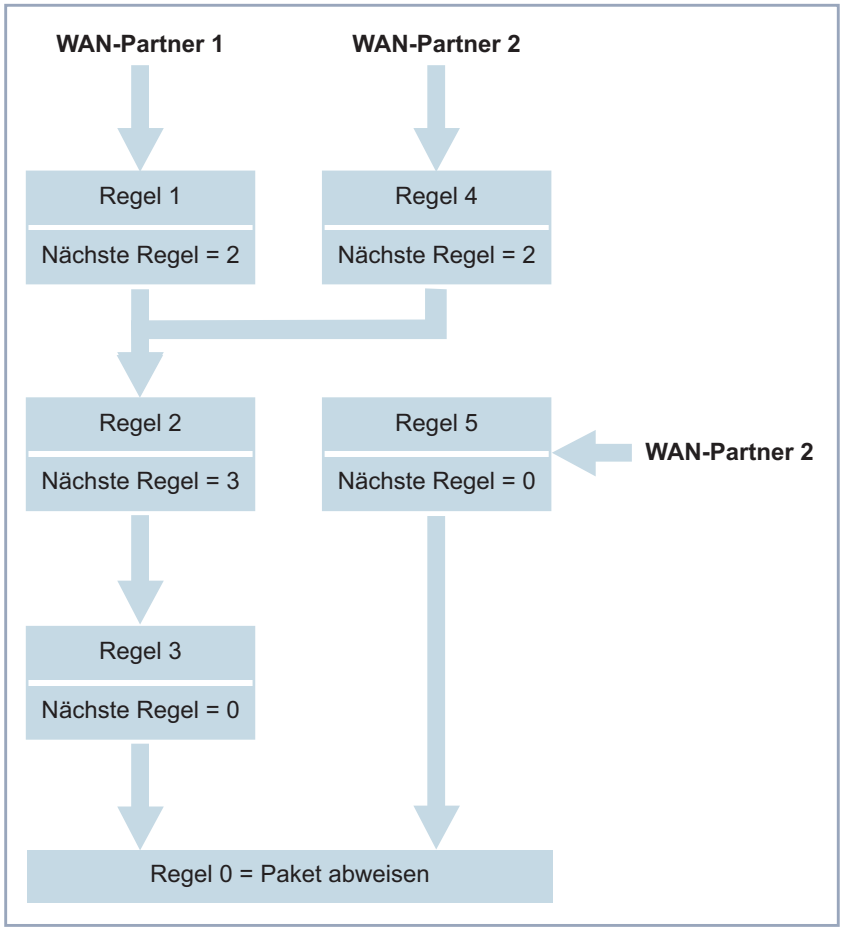


Bild 8-4: Regelketten für unterschiedliche Schnittstellen

Die Konfiguration erfolgt in:

- ***IP*** ➧ ***ACCESS LISTS*** ➧ ***FILTER***
- ***IP*** ➧ ***ACCESS LISTS*** ➧ ***RULES***
- ***IP*** ➧ ***ACCESS LISTS*** ➧ ***RULES*** ➧ **REORG**
- ***IP*** ➧ ***ACCESS LISTS*** ➧ ***INTERFACES***

In ***IP*** ➧ ***ACCESS LISTS*** ➧ ***FILTER*** definieren Sie Filter:

Feld	Bedeutung
Description	Bezeichnung des Filters. Beachten Sie, daß in anderen Menüs evtl. nur die ersten 15 Zeichen angezeigt werden.
Index	Kann nicht verändert werden. **BinGO!** vergibt hier neu definierten Filtern automatisch eine Nummer.
Protocol	Legt ein Protokoll fest. Mögliche Werte: *any*, *icmp*, *ggp*, *tcp*, *egp*, *pup*, *udp*, *hmp*, *xns_idp*, *rdp*, *rsvp*, *gre*, *esp*, *ah*, *igrp*, *ospf*, *l2tp*. *any* paßt auf jedes Protokoll, *tcp* paßt nur auf TCP-Datenpakete, usw.
Connection State	Bei *Protocol* = *tcp* können Sie ein Filter definieren, das auf dem Status der TCP-Verbindung basiert. Mögliche Werte: *established:* Das Filter paßt auf alle TCP-Pakete, die beim Routing über **BinGO!** keine neue Verbindung öffnen würden. *any:* Das Filter paßt auf alle TCP-Pakete.
Type	Nur bei *Protocol* = *icmp*. Mögliche Werte: *any*, *echo reply*, *destination unreachable*, *source quench*, *redirect*, *echo*, *time exceeded*, *param problem*, *timestamp*, *timestamp reply*, *address mask*, *address mask reply* . Siehe RFC 792.
Source / Destination Address	(optional) Quell- bzw. Ziel-IP-Adresse der Datenpakete, auf die das Filter paßt.
Source / Destination Mask	(optional) Quell- bzw. Ziel-Netzmaske. Durch die Kombination von *Address* und *Mask* wird ein Bereich von IP-Adressen beschrieben, auf den das Filter paßt.
Source / Destination Port	Port-Nummer bzw. Bereich von Port-Nummern, auf die das Filter paßt.

Feld	Bedeutung
Specify Port	Nur bei *Source / Destination Port* = *specify* bzw. *specify range:* Bereich von Port-Nummern eingeben.

Tabelle 8-9: ***IP*** ➧ ***ACCESS LISTS*** ➧ ***FILTER***

Die Felder *Source Port* bzw. *Destination Port* enthalten folgende Auswahlmöglichkeiten:

Mögliche Werte	Bedeutung
any	Das Filter paßt auf alle ➤➤ **Port**-Nummern.
specify	Ermöglicht Eingabe einer Port-Nummer unter *Specify Port*.
specify range	Ermöglicht Eingabe eines Bereiches von Port-Nummern unter *Specify Port*.
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 8-10: *Source Port* bzw. *Destination Port*

Port-Nummern Port-Nummern sind wie folgt verteilt:

<table>
<tr><th>0 ... 1023</th><th>1024 ... 4999</th><th>5000 ... 32767</th><th>32768 ... 65535</th></tr>
<tr><td>Well Known Ports,
d. h. fest vergeben.</td><td colspan="3">Die Ports werden von ➤➤ Clients bzw.
➤➤ Servern dynamisch angelegt und haben keine feste Bedeutung (mit Ausnahme von besonderen Vereinbarungen):
unpriv (1024..65535)</td></tr>
<tr><td>priv (0..1023)</td><td>clients 1
(1024..4999)</td><td>server
(5000..32767)</td><td>clients 2
(32768..65535)</td></tr>
</table>

Tabelle 8-11: Bereiche von Portnummern

Im Folgenden eine Übersicht über einige häufig gebrauchte Port-Nummern mit den zugewiesenen Diensten:

Dienst	Protokoll	Port-Nummer
File Transfer Protocol (➤➤ **FTP**) (Daten)	TCP	20
File Transfer Protocol (FTP) (Kommandos)	TCP	21
Telnet	TCP	23
Simple Mail Transfer Protocol (SMTP)	TCP	25
Domain Name Server (➤➤ **DNS**)	TCP, UDP	53
Trivial File Transfer Protocol (➤➤ **TFTP**)	UDP	69
http/WWW	TCP	80
POP3 (E-Mail-Abfrage)	TCP	110
Network Time Protocol	TCP, UDP	119
➤➤ **NetBIOS**-Name (NBNAME)	UDP	137
NetBIOS Datagram (NBDATA)	UDP	138
NetBIOS Session (NBSESSION)	TCP	139
Simple Management Network Protocol (SNMP)	UDP	161
SNMP (Traps)	UDP	162
Syslog Service (SYSLOG)	UDP	514
Network File System	UDP	2049
Remote-CAPI	TCP	2662
Remote-TAPI	TCP	2663

Tabelle 8-12: Dienste und Port-Nummern

Beispiel Als Beispiel soll eine vereinfachte FTP-Verbindung verdeutlichen, wie Quell- und Ziel-Ports zu verwenden sind: Neben Quell- und Ziel-IP-Adressen verwendet das IP-Protokoll auch Quell- und Ziel-Port-Nummern, um Datenverbindungen eindeutig zu identifizieren. Der FTP-Client erzeugt eine Nummer, z. B. xyz, die als Quell-Port-Nummer verwendet wird. Als Ziel-Port-Nummer verwendet er die Nummer, unter der der FTP-Server den Dienst FTP anbietet, also z. B. 21. Der FTP-Server versendet dann IP-Pakete, die als Quell-Port-Nummer die 21 und als Ziel-Port-Nummer die xyz verwenden:

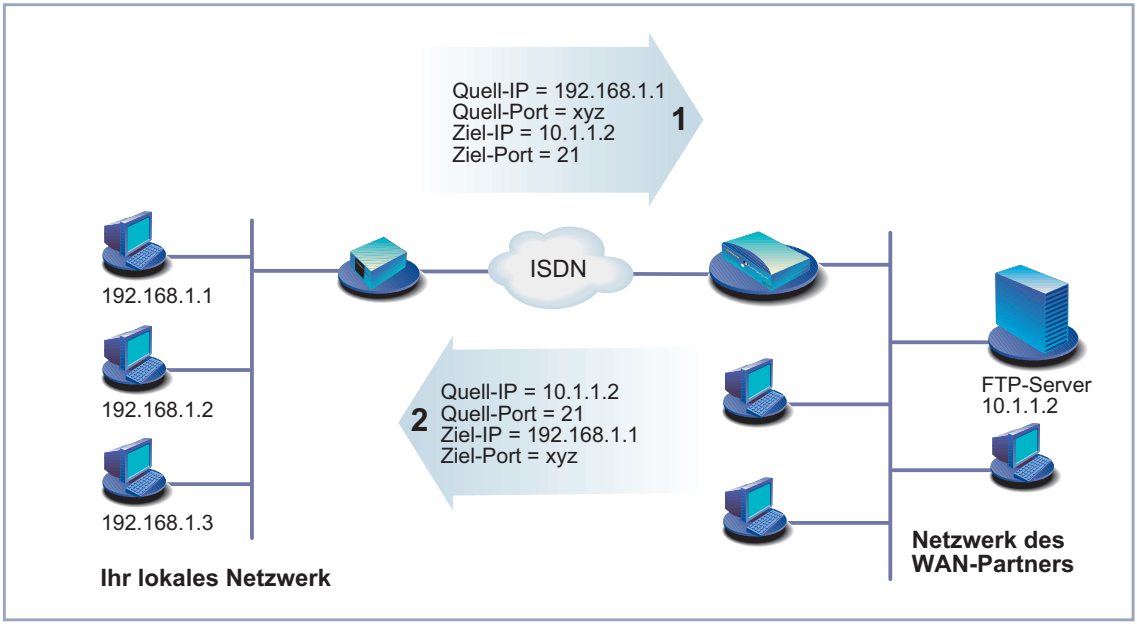


Bild 8-5: Beispiel: FTP-Verbindung

In ***IP*** ➧ ***ACCESS LISTS*** ➧ ***RULES*** definieren Sie Regeln:

Feld	Bedeutung
Index	Kann nicht verändert werden. **BinGO!** vergibt hier neu definierten Regeln automatisch eine Nummer bzw. zeigt *Index* von bestehenden Regeln an.
Insert behind Rule	Erscheint nur, wenn eine neue Regel definiert wird. Legt fest, nach welcher Regel die neue Regel eingefügt wird. Mit *none* beginnen Sie eine neue eigenständige Kette.
Action	Legt fest, wie mit einem ausgefilterten Datenpaket verfahren wird.
Filter	Filter, das verwendet wird.
Next Rule	Erscheint nur, wenn eine bestehende Regel editiert wird. Legt fest, welche Regel als nächstes angewendet wird.

Tabelle 8-13: ***IP*** ➧ ***ACCESS LISTS*** ➧ ***RULES***

Das Feld *Action* enthält folgende Auswahlmöglichkeiten:

Mögliche Werte	Bedeutung
allow M	Paket durchlassen, wenn das Filter paßt.
allow !M	Paket durchlassen, wenn das Filter nicht paßt.
deny M	Paket abweisen, wenn das Filter paßt.
deny !M	Paket abweisen, wenn das Filter nicht paßt.
ignore	Nächste Regel anwenden.

Tabelle 8-14: *Action*

Im Untermenü ***IP*** ➧ ***ACCESS LISTS*** ➧ ***RULES*** ➧ **REORG** können Sie die Reihenfolge der Regeln in einer Kette verändern:

Feld	Bedeutung
Index of Rule that gets Index 1	Legt Regel fest, die an erster Stelle der Kette stehen soll.

Tabelle 8-15: ***IP*** ➧ ***ACCESS LISTS*** ➧ ***RULES*** ➧ **REORG**

Wenn Sie so eine Kette neuorganisieren, verbindet **BinGO!** nach Auswahl von *Index of Rule that gets Index 1* die verbleibenden Regeln neu:

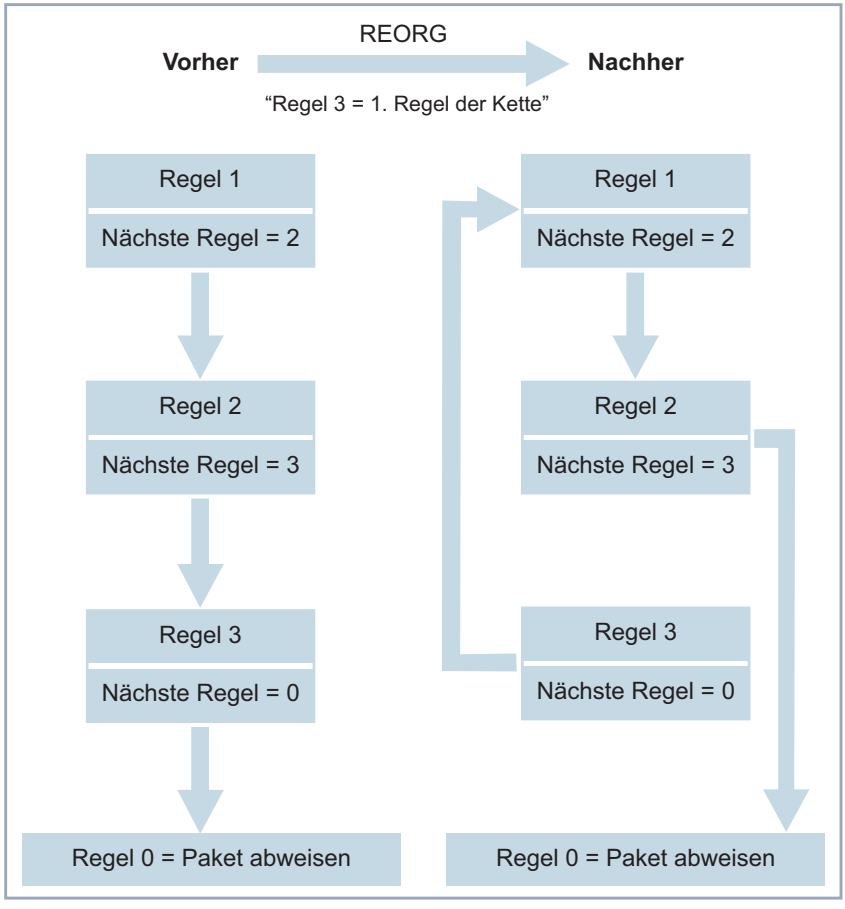


Bild 8-6: Beispiel für die Neuorganisation einer Kette

In ***IP*** ➧ ***ACCESS LISTS*** ➧ ***INTERFACES*** legen Sie fest, welche Schnittstelle mit welcher Regel beginnt:

Standardmäßig wird immer die Regel mit *Index = 1* für eine neuerstellte Schnittstelle (z. B. zu einem WAN-Partner) als erste Regel angewendet.

Feld	Bedeutung
Interface	**BinGO!**-Schnittstelle
First Rule	Legt fest, welche Regel als erstes für Datenpakete, die über *Interface* **BinGO!** erreichen, angewendet wird. Mit *none* legen Sie fest, daß für *Interface* keine Filter angewendet werden.

Tabelle 8-16: ***IP*** ➧ ***ACCESS LISTS*** ➧ ***INTERFACES***

ToDo Gehen Sie folgendermaßen vor, um Filter und Regeln zu definieren:

Achten Sie darauf, daß Sie sich beim Konfigurieren der Filter nicht selbst "aussperren". Wenn Sie z. B. das erste Filter mit einer Regel verknüpfen, die *Action* = *Allow M* ausführt, kommt wirklich nur durch, was Sie mit dem Filter ausdrücklich erlaubt haben. So kann es leicht passieren, daß Ihr Zugriff auf **BinGO!** mit telnet nicht mehr gestattet wird, sobald Sie das Filter eintragen und mit **SAVE** bestätigen.

- Verwenden Sie keine Filter auf dem LAN-Interface (*First Rule* = *none*), wenn Sie über telnet auf **BinGO!** zugreifen.
- Wenn Sie über die serielle Schnittstelle oder ISDN-Login auf **BinGO!** zugreifen, passiert Ihnen zumindest während der Konfiguration nichts.

Filter

- Gehen Sie zu ***IP*** ➧ ***ACCESS LISTS*** ➧ ***FILTERS***.
- Fügen Sie mit **ADD** einen neuen Eintrag hinzu oder wählen Sie einen bestehenden Eintrag aus und bestätigen mit der **Eingabetaste**, um ihn zu verändern.
- Geben Sie *Description* ein.
- Wählen Sie *Protocol* aus.
- Geben Sie gegebenenfalls *Source Address* ein.
- Geben Sie gegebenenfalls *Source Mask* ein.
- Wählen Sie *Source Port* aus.
- Geben Sie gegebenenfalls *Specify Port* ein.
- Geben Sie gegebenenfalls *Destination Address* ein.

- Geben Sie gegebenenfalls *Destination Mask* ein.
- Wählen Sie *Destination Port* aus.
- Geben Sie gegebenenfalls *Specify Port* ein.
- Bestätigen Sie mit **SAVE**.
- Wiederholen Sie diese Schritte so oft, bis Sie alle gewünschten Filter definiert haben.

Vergessen Sie nicht, gegebenenfalls ein Filter für die Freigabe der restlichen Datenpakete zu definieren (*Protocol* = *any*, *Source Port* = *any*, *Destination Port* = *any*).

- Verlassen Sie ***IP*** ➧ ***ACCESS LISTS*** ➧ ***FILTERS*** mit **EXIT**.

Regeln

- Gehen Sie zu ***IP*** ➧ ***ACCESS LISTS*** ➧ ***RULES***, um die Filter mit Regelketten miteinander zu verbinden.
- Fügen Sie mit **ADD** einen neuen Eintrag hinzu oder wählen Sie einen bestehenden Eintrag aus und bestätigen mit der **Eingabetaste**, um ihn zu verändern.
- Wählen Sie *Insert behind Rule aus*, wenn Sie eine neue Regel erstellen.
- Wählen Sie *Action* aus.
- Wählen Sie *Filter* aus.
- Wählen Sie *Next Rule* aus, wenn Sie eine bestehende Regel verändern.
- Bestätigen Sie mit **SAVE**.
- Wiederholen Sie diese Schritte so oft, bis Sie alle gewünschten Regeln definiert haben.

Vergessen Sie nicht, gegebenenfalls als letzte Regel in der Kette eine Regel für die Freigabe der restlichen Datenpakete zu definieren (*Action* = *allow M*).

Mit *Insert behind Rule* = *none* können Sie eine neue Regelkette eröffnen.

- Verlassen Sie ***IP*** ➧ ***ACCESS LISTS*** ➧ ***RULES*** mit **EXIT**.

Schnittstelle

- Gehen Sie zu ***IP*** ➧ ***ACCESS LISTS*** ➧ ***INTERFACES***.
- Wählen Sie eine Schnittstelle aus und bestätigen mit der **Eingabetaste**, wenn Sie eine andere als die angezeigte Regel als erste Regel für diese Schnittstelle verwenden wollen.
- Wählen Sie *First Rule* aus.
- Bestätigen Sie mit **SAVE**.

Kette neu organisieren

Gehen Sie folgendermaßen vor, um eine bestehende Kette von Regeln neu zu organisieren:

- Gehen Sie zu ***IP*** ➧ ***ACCESS LISTS*** ➧ ***RULES*** ➧ **REORG**.
- Wählen Sie *Index of Rule that gets Index 1* aus.
- Bestätigen Sie mit **REORG**.

Wenn Sie in Ihrem Netzwerk mit Windows arbeiten, ist es meistens sinnvoll, ein NetBIOS-Filter zu definieren. Dieses Konfigurationsbeispiel finden Sie in Kapitel 6.1.6, Seite 145 Schritt für Schritt erläutert.

8.2.9 Lokale Filter

Der Zugang zu den lokalen Diensten auf **BinGO!** (telnet, ➤➤ **CAPI**, trace, usw.) kann über eine eigene MIB-Tabelle geregelt werden. Solange diese leer ist, sind über alle Schnittstellen Zugriffe auf die lokalen Dienste möglich, sofern dies nicht durch Einsatz von NAT (siehe Kapitel 8.2.7, Seite 252) oder globalen Filtern (siehe Kapitel 8.2.8, Seite 258) verboten wurde.

Lokale Filter sind also ein zusätzliches Instrument, das aber einfacher zu handhaben ist als die globalen Filter und zudem die Performance beim normalen Routing nicht beeinträchtigt.

Aktivieren Sie lokale Filter durch Einträge in den MIB-Tabellen **localTcpAllowTable** und **localUdpAllowTable**.

8.2.10 Backroute Verification

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

ToDo

Gehen folgendermaßen vor, um Backroute Verification für einen WAN-Partner zu aktivieren:

- Gehen Sie zu ***WAN Partner*** ➧ ***Edit*** ➧ ***IP*** ➧ ***Advanced Settings***.
- Aktivieren Sie *Back Route Verify* mit *on*.
- Bestätigen Sie mit **OK**.

8.2.11 TAF-Client

Personenbezogene Authentisierung

Die Funktion Token Authentication Firewall (TAF) ermöglicht eine personenbezogene Authentisierung von IP-Verbindungspartnern. BinTec's Lösung integriert dazu die Mechanismen der Token-Authentisierung von Security Dynamics und erlaubt Datenpaketen die Überquerung des Routers erst nach Abschluß einer erfolgreichen Authentisierung der zugehörigen Source-Adresse.

Auf BinTec's Corporate Access Routern können Sie diese Funktion freischalten und den Router als TAF-Server einrichten. Den Personal Access Router **BinGO!** können Sie als TAF-➤➤ **Client** konfigurieren und sich so auf einem TAF-Server und dem angeschlossenen LAN Zugang verschaffen (wenn der TAF-Server entsprechend eingerichtet wurde). Die genaue Darstellung der

Funktionsweise und die erforderlichen Konfigurationsschritte finden Sie in BRICKware for Windows.

8.2.12 Extended IP-Routing (XIPR)

Ergänzend zu der normalen Routing-Tabelle kann **BinGO!** auch Routingentscheidungen aufgrund einer zusätzlichen Tabelle, der Extended Routing-Tabelle, treffen. Dabei kann **BinGO!** neben der Zieladresse 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 bestehen, werden diese gebenüber den Einträgen in der normalen Routing-Tabelle bevorzugt behandelt.

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

Die Konfiguration erfolgt in der MIB-Tabelle **ipExtRtTable**. Eine ausführliche Beschreibung finden Sie in der Software Reference.

8.3 Abhörsicherung

Für die Datensicherheit von PPP-Verbindungen auf sicherheitskritischen Verbindungen können Sie einen Verschlüsselungsmechanismus einsetzen, wenn beide Verbindungspartner diesen unterstützen.

8.3.1 Verschlüsselung

BinGO! unterstützt Verschlüsselung von PPP-Verbindungen mit WAN-Partnern. Dabei wird das Verfahren ➤➤ **MPPE** (Microsoft Point to Point ➤➤ **Encryption**) mit Schlüssellängen von 40 bit bzw. 128 bit eingesetzt.

Die Konfiguration erfolgt in ***WAN PARTNER*** ➧ ***EDIT***:

Feld	Bedeutung
Encryption	Legt die Art der Verschlüsselung fest. Mögliche Werte: ■ *MPPE 40:* Schlüssellänge 40 bit ■ *MPPE 128:* Schlüssellänge 128 bit ■ *none:* keine Verschlüsselung

Tabelle 8-17: ***WAN PARTNER*** ➧ ***EDIT***

ToDo Gehen Sie folgendermaßen vor, um Verschlüsselung einzustellen:

➤ Gehen Sie zu ***WAN PARTNER***.

➤ Wählen Sie einen WAN-Partner aus und bestätigen Sie mit der **Eingabetaste**, um die PPP-Verbindungen mit diesem Partner zu verschlüsseln.

➤ Wählen Sie *Encryption* aus, z. B. *MPPE 40*.

➤ Bestätigen Sie mit **SAVE**.

8.3.2 VPN (mit Zusatzlizenz)

Mit Hilfe von PPTP (Point to Point Tunneling Protocol) kann **BinGO!** ein VPN (Virtual Private Network) herstellen. Dies dient zu einer sicheren (verschlüsselten) Übertragung von Daten über WAN-Verbindungen, z. B. über das Internet. So kann z. B. von Außendienstmitarbeitern per Laptop ein Zugang auf Daten des Firmennetzes kostengünstig über das Internet realisiert werden (Einwahl über einen örtlichen Internet Service Provider).

Detaillierte Informationen und Konfigurationshinweise (mit Beispielen) finden Sie in der Extended Feature Reference.

8.4 Besonderheiten

8.4.1 Startup-Verhalten

BinGO! nimmt seine Routingtätigkeiten erst auf, wenn die komplette Konfiguration, insbesondere auch die definierten Filter, geladen sind. Somit ist es nicht möglich, durch Provokation eines Systemstarts einen Zwischenzustand des Systems auszunutzen, in dem vielleicht schon geroutet wird, aber noch keine Filter aktiv sind.

8.4.2 Auto-Logout

Verbindung zu **BinGO!** über telnet, ➤➤ **isdnlogin** oder seriell werden automatisch getrennt, wenn 15 Minuten lang keine Eingabe über die Tastatur erfolgt. Damit wird das Auslesen oder Ändern der Systemkonfiguration auf "vergessenen" Verbindungen erschwert. Den Zeitraum können Sie mit dem Kommando `t <Zeit in Sekunden>` verändern (siehe Kapitel 12.1, Seite 316).

8.4.3 Vorbeugung gegen Denial-of-Service-Attaken

Eine Denial-of-Service-Attacke (DoS) zielt darauf ab, durch Senden bestimmter Pakete ein System zu blockieren oder zum Neustarten zu bringen. Damit kann das System oder ein bestimmter Dienst nicht mehr genutzt werden. Es gibt mehrere Möglichkeiten dies zu bewerkstelligen, z. B. durch Senden eines übergroßen Ping-Paketes oder durch Ersetzen der Quelladresse eines gesendeten Paketes mit der Zieladresse.

Einige DoS-Attacken auf den Router selbst werden bereits durch die interne Codierung unterbunden.

Z. B. existiert an allen **BinGO!**-Schnittstellen, für die Sie Network Address Translation (NAT) aktivieren, ein Schutz für die angeschlossenen Rechner gegen einige DoS-Attacken mit fragmentierten Paketen. Die Paketfragmente wer-

den beim Durchgang durch NAT wieder zusammengefügt, bevor das Paket den Router passieren kann.

Einige DoS-Angriffe, die mit gefälschten Quell-IP-Adressen arbeiten, können Sie gegebenenfalls mit Hilfe der Funktion Backroute Verification verhindern (siehe Kapitel 8.2.10, Seite 271).

DoS-Angriffen, die auf Systemstörung durch Überlaufen von Logdateien (Syslog-Messages) spekulieren, können Sie durch geeignete Plazierung und Größenlimitierung dieser Dateien begegnen.

8.5 Checkliste

Die nachfolgende Liste gibt die wichtigsten sicherheitskritischen Punkte an, die Sie bei der Konfiguration von **BinGO!** beachten sollten:

- Haben Sie alle vier Paßwörter für den Systemzugang (admin, read, write, http) verändert? Siehe Kapitel 6.1.2, Seite 128.
- Werden die Aktivitäten von **BinGO!** auf mindestens einem externen Rechner ausreichend genau protokolliert und überprüfen Sie die Syslog-Messages regelmäßig? Siehe Kapitel 8.1.1, Seite 236.
- Haben Sie den Zugriff auf die lokalen Dienste und Ressourcen eingeschränkt auf bekannte Rechner oder Netze? Insbesondere die Zugänge per CAPI, SNMP, HTTP, Trace und Telnet sollten Sie nur bekannten Rechnern gestatten.
- Liegen per TFTP abgespeicherte Konfigurationsdateien an einem sicheren Ort?
- Haben Sie alle PPP-Zugänge mit Paßwort gesichert?
- Haben Sie für die Verbindung zum Internet Service Provider (ISP) Network Address Translation (NAT) aktiviert? Siehe Kapitel 8.2.7, Seite 252.
- Haben Sie an kritischen Schnittstellen den IP-Datenverkehr ggf. mit Hilfe von Filtern geregelt und IP-Address-Spoofing verhindert? Dabei sollten Sie besonders die Schnittstellen beachten, die Sie nicht durch NAT abgesichert haben! Siehe Kapitel 8.2.8, Seite 258.
- Haben Sie den Zugang über ISDN-Login für Fernwartung gesperrt? Haben Sie einen Eintrag unter ***CM-1BRI, ISDN S0*** ➧ ***INCOMING CALL ANSWERING*** gemacht? Siehe Kapitel 6.1.4, Seite 133.

Als zusätzliche Punkte sollten Sie beachten:

- Verwenden Sie für PPP-Verbindungen Callback nach dem Microsoft-Verfahren? Beachten Sie bitte die Hinweise in Kapitel 8.2.4, Seite 250.
- Setzen Sie auf sicherheitskritischen Verbindungen ein Verschlüsselungsprotokoll zur Abhörsicherung ein? Siehe Kapitel 8.3.1, Seite 273.

- Setzen Sie auf sicherheitskritischen Verbindungen eine personenbezogene Authentisierung ein?
- Erlauben Sie die Beeinflussung durch Routing-Protokolle (z. B. RIP) nur an vertrauenswürdigen Netzen? Siehe Kapitel 7.2.6, Seite 210.
- Kontrollieren Sie, welche Rechner Zugang auf die Remote-CAPI-Schnittstelle haben, welche Applikationen darauf verwendet werden und ob die Verbindungen, die mit diesen Applikationen verwendet werden, erwünscht sind. Nutzen Sie das CAPI-User-Konzept?
- Sind eventuell zusätzlich angelegte Benutzeraccounts unproblematisch?
- Haben Sie das Abhören von Verbindungen auf dem Ethernet durch eine geeignete LAN-Infrastruktur verhindert?

9 Konfigurationsmanagement

In diesem Kapitel finden Sie Hinweise zum Verwalten Ihrer Konfigurationsdateien und zum Updaten der Software von **BinGO!**. Es umfaßt folgende Bereiche:

- Verwalten der Konfigurationsdateien:
  - Wo sind die Konfigurationsdateien?
  - Was ist Flash und Memory?
  - Wie kann ich mit Konfigurationsdateien umgehen?
- Software-Update durchführen
  - Wie bleibe ich immer auf dem neuesten Stand?
  - Wie lade ich ein neues Boot-Image?

9.1 Konfigurationsdateien verwalten

Flash **BinGO!** liest seine Konfigurationsinformationen aus Konfigurationsdateien. Diese Konfigurationsdateien sind gespeichert im Flash EEPROM (electronically eraseable programmable read-only memory) von **BinGO!**. Im Flash-Speicher können einige verschiedene Konfigurationsdateien gespeichert werden. Auch wenn **BinGO!** ausgeschaltet ist, bleiben die Daten im Flash gespeichert.

Memory Im Arbeitsspeicher (Memory bzw. RAM) befindet sich die aktuelle Konfiguration und alle Änderungen, die Sie während des Betriebes auf **BinGO!** einstellen. Der Inhalt von Memory geht verloren, wenn **BinGO!** ausgeschaltet wird. Wenn Sie Ihre Konfiguration ändern und diese Änderungen auch beim nächsten Start von **BinGO!** beibehalten wollen, müssen Sie die gänderte Konfiguration vor dem Ausschalten im Flash speichern: **Exit ➧ Save as boot configuration and exit** (siehe Kapitel 6.3, Seite 187). Diese Datei wird damit als Boot-Konfigurationsdatei mit dem Namen "boot" im Flash gespeichert. Beim Starten von **BinGO!** wird dann genau diese Datei, also die Konfigurationsdatei mit dem Namen "boot", im Memory geladen und damit wirksam.

Aktionen Stellen Sie sich den Flash-Speicher als Verzeichnis von Konfigurationsdateien vor. Die Dateien in diesem Verzeichnis können kopiert, verschoben, gelöscht und neu angelegt werden. Es ist auch möglich, Konfigurationsdateien zwischen **BinGO!** und einem Remote-Host per TFTP zu transferieren.

Windows Unter Windows können Sie dafür den TFTP-Server der **DIME Tools** verwenden (siehe BRICKware for Windows). So können Sie z. B. eine Konfigurationsdatei von **BinGO!** auf Ihrem lokalen Rechner abspeichern.

Die mit dem TFTP-Server der DIME Tools zu transferierenden Dateien dürfen maximal aus 8 Zeichen bestehen (+ maximal 3 Zeichen als Anhang), z. B. bingo.cf.

Unix Unter Unix ist ein TFTP-Server Teil des Systems, beachten Sie bitte die Hinweise in der Software Reference.

Mit Hilfe des Setup Tools können Sie die verschiedenen Aktionen ausführen:

➤ Gehen Sie in das Menü ***CONFIGURATION MANAGEMENT***.

```
BinGO! Setup Tool                                BinTec Communications AG
                                                                 MyBinGO!

    Operation                    get  (TFTP --> FLASH)

    TFTP Server IP Address       192.168.1.1
    TFTP File Name               brick.cf

    Name in Flash                boot

    Type of last operation       get (TFTP --> FLASH)
    State of last operation      done

        START OPERATION                          EXIT

Use <Space> to select
```

Das Menü enthält folgende Felder:

Feld	Bedeutung
Operation	Aktion, die Sie ausführen möchten.
TFTP Server IP Address	Die IP-Adresse oder der Hostname (falls der Hostname aufgelöst werden kann) des TFTP-Servers von bzw. zu dem Sie eine Konfigurationsdatei transferieren wollen.
TFTP File Name	Name der Konfigurationsdatei auf dem TFTP-Server (ohne Pfadangabe).
Name in Flash	Name der Konfigurationsdatei im Flash.
New Name in Flash	Name der neu zu erzeugenden Konfigurationsdatei im Flash (bei *Operation* = *move* oder *copy*).
Type of last operation	Vorhergehende Aktion (seit dem letzten **BinGO!**-Start).
State of last operation	Status der letzten Aktion.

Tabelle 9-1: ***CONFIGURATION MANAGEMENT***

Das Feld *Operation* enthält folgende Auswahlmöglichkeiten:

Mögliche Werte	Bedeutung
save (MEMORY --> FLASH)	Alle aktuellen Einstellungen von Memory ins Flash als Konfigurationsdatei <Name in Flash> speichern. <Name in Flash> wird dabei überschrieben bzw. neu erzeugt.
load (FLASH --> MEMORY)	Konfigurationsdatei <Name in Flash> vom Flash ins Memory laden. Die Einstellungen von <Name in Flash> werden sofort wirksam.
move (FLASH --> FLASH)	Konfigurationsdatei <Name in Flash> in <New Name in Flash> umbenennen.
copy (FLASH --> FLASH)	Konfigurationsdatei <Name in Flash> als <New Name in Flash> kopieren.
delete (FLASH)	Konfigurationsdatei <Name in Flash> löschen.
put (FLASH --> TFTP)	Konfigurationsdatei <Name in Flash> aus dem Flash zum TFTP-Host mit der IP-Adresse <TFTP Server IP Address> transferieren. <TFTP File Name> wird dabei auf dem TFTP-Host mit Inhalt von <Name in Flash> überschrieben oder neu erzeugt. <TFTP File Name> wird im ASCII-Format gespeichert und kann editiert werden.
get (TFTP --> FLASH)	Konfigurationsdatei <TFTP File Name> von TFTP-Host mit der IP-Adresse <TFTP Server IP Address> ins Flash transferieren. <Name in Flash> wird dabei mit Inhalt von <TFTP File Name> überschrieben oder neu erzeugt. Da die Konfigurationsdatei ins Flash und nicht ins Memory transferiert wird, ist anschließend das Ausführen von load (FLASH --> MEMORY) erforderlich, damit die Einstellungen auf **BinGO!** wirksam werden.

Mögliche Werte	Bedeutung
state (MEMORY --> TFTP)	Alle aktuellen Einstellungen im Memory als <TFTP File Name> auf TFTP-Host mit der IP-Adresse <TFTP Server IP Address> speichern. <TFTP File Name> wird dabei überschrieben oder neu erzeugt.
reboot	**BinGO!** neu starten. Einstellungen im Memory gehen werden durch Einstellungen von boot aus Flash ersetzt.

Tabelle 9-2: *Operation*

Das Feld *State of last operation* kann folgendes anzeigen:

Mögliche Werte	Bedeutung
todo	Die Aktion wurde noch nicht gestartet.
running	Die Aktion wird gerade ausgeführt.
done	Die Aktion wurde erfolgreich ausgeführt.
error	Die Aktion konnte nicht vollständig ausgeführt werden (siehe Syslog-Message).

Tabelle 9-3: *State of last operation*

Wenn beim Ausführen der Aktion *get (TFTP --> FLASH)* ein Fehler auftritt und die Aktion abgebrochen wird, ist die zu überschreibende Datei im Flash gelöscht. Wenn Sie also eine Datei "boot" transferieren, wird in diesem Fall **BinGO!**s Boot-Datei gelöscht, **BinGO!** kann beim Hochfahren keine Konfiguration mehr laden. Benennen Sie gegebenenfalls die zu transferierende Datei um!

Für Ausführen von *put (Flash --> TFTP)*, *get (TFTP --> Flash)* und *state (MEMORY --> TFTP)* benötigen Sie einen TFTP-Server auf dem Host, zu oder von dem Sie eine Konfigurationsdatei transferieren wollen.
Wenn der TFTP-Host ein Windows-PC ist, klicken Sie auf **Programme** ➧ **BRICKware** ➧ **DIME Tools** im Windows-Startmenü, um die **DIME Tools** zu öffnen und aktivieren Sie den TFTP-Server mit **File** ➧ **TFTP Server**, bevor Sie die entsprechende Aktion durchführen.

Wenn Sie Ihren Windows-PC als TFTP-Host nutzen wollen, aber nicht sicher sind, wie die IP-Adresse des PCs lautet, gehen Sie folgendermaßen vor:

Windows 95:

- Klicken Sie im Windows-Startmenü auf **Ausführen**.
- Geben Sie `winipcfg` ein.

  Es erscheint ein Fenster, in dem Sie die IP-Adresse Ihres Rechner und andere Netzinformationen sehen.

Windows NT:

- Klicken Sie im Windows-Startmenü auf **Programme** ➧ **Eingabeaufforderung**.
- Geben Sie `ipconfig` oder `ipconfig/all` ein, um Ihre IP-Adresse Ihres Rechners und andere Netzinformationen abzufragen.

Aktion ausführen

Gehen Sie folgendermaßen vor, um eine Aktion auszuführen:

- Wählen Sie *Operation* aus.
- Aktivieren Sie einen TFTP-Server, falls Sie als *Operation put*, *get* oder *state* ausgewählt haben.
- Wählen Sie in ***CONFIGURATION MANAGEMENT*** die erforderlichen Einstellungen aus bzw. tragen Sie die erforderlichen Werte ein.
- Wählen Sie **START OPERATION** aus und bestätigen Sie mit der **Eingabetaste**.

  Solange die Aktion ausgeführt wird, erscheint in der Hilfszeile des Setup Tool *OPERATING*, *State of last operation* zeigt *running* an.

  Wenn die Aktion erfolgreich ausgeführt wurde, wird sie unter *Type of last operation* angezeigt, *State of last operation* nimmt den Wert *done* an.

Wenn unter *State of last operation error* angezeigt wird, überprüfen Sie Ihre Einstellungen:

- Haben Sie unter TFTP Server IP Address eine falsche IP-Adresse angegeben?
- Besteht der Name der Konfigurationsdatei aus mehr als 8 Zeichen und die Extension aus mehr als 3 Zeichen (bei Verwendung der DIME Tools)?
- Unterstützt der Host nicht TFTP (haben Sie vergessen, vor Ausführen der Aktion den TFTP-Server der DIME Tools zu starten)?
- Liegt die Quelldatei nicht im konfigurierten Verzeichnis des TFTP-Pfades der DIME Tools (Bei *Operation* = *get*)? Beachten Sie BRICKware for Windows, um den TFTP-Pfad zu verändern.
- Wenn diese Punkte nicht zutreffen, gehen Sie folgendermaßen vor, um die Fehlerursache zu finden:

➤ Verlassen Sie das Setup Tool.

➤ Geben Sie in der SNMP-Shell ein: `debug config &`.

➤ Öffnen Sie erneut das Setup Tool mit `setup`.

➤ Führen Sie die gewünschte Aktion in ***CONFIGURATION MANAGEMENT*** aus.

In der Hilfszeile des Setup Tool Menüs wird bei Auftreten eines Fehlers eine Fehlermeldung mit der Ursache angezeigt.

➤ Beseitigen Sie die Ursache des Problems und führen Sie die Aktion erneut aus.

➤ Verlassen Sie ***CONFIGURATION MANAGEMENT*** mit **EXIT**.

Beispiel Sie haben die Konfigurationsdatei brick.cf erstellt, z. B. mit Hilfe des Configuration Wizard. Sie haben die Datei nicht über die serielle Schnittstelle auf **BinGO!** übertragen lassen, brick.cf liegt im Verzeichnis C:\BRICK auf Ihrem Rechner. Ihr Rechner hat die IP-Adresse 192.168.1.1. Wenn Sie brick.cf von Ihrem Rechner auf **BinGO!** transferieren wollen, gehen Sie folgendermaßen vor:

➤ Windows-PC: Klicken Sie auf **Programme** ➧ **BRICKware** ➧ **DIME Tools** im Windows-Startmenü, um **DIME Tools** zu starten. Der TFTP-Server muß aktiv sein.

- Aktivieren eines TFTP-Servers unter Unix: siehe Software Reference.
- Gehen Sie zu ***CONFIGURATION MANAGEMENT***.

TFTP-Host --> Flash

- Wählen Sie *Operation* aus: *get (TFTP --> FLASH)*.
- Tragen Sie *TFTP Server IP Address* ein, z. B. *192.168.1.1*.
- Tragen Sie *TFTP File Name* ein: *brick.cf*.
- Tragen Sie *Name in Flash* ein, z. B. *boot*.
- Wählen Sie **START OPERATION** aus und bestätigen Sie mit der **Eingabetaste**.

  *S*olange die Aktion ausgeführt wird, erscheint in der Hilfszeile des Setup Tool *OPERATING*, *State of last operation* zeigt *running* an.

  Wenn die Aktion erfolgreich ausgeführt wurde, wird unter *Type of last operation get (TFTP --> FLASH)* angezeigt, *State of last operation* nimmt den Wert *done* an.

  Die Konfigurationsdatei brick.cf ist z. B. unter dem Namen boot im Flash von **BinGO!** gespeichert.

Gehen Sie anschließend folgendermaßen vor, um die Einstellungen von brick.cf sofort auf **BinGO!** wirksam werden zu lassen:

Flash --> Memory

- Wählen Sie erneut *Operation* aus: *load (FLASH --> MEMORY)*.
- Wählen Sie *Name in Flash* aus, z. B. *boot*.
- Wählen Sie **START OPERATION** aus und bestätigen Sie mit der **Eingabetaste**.

  *S*olange die Aktion ausgeführt wird, erscheint in der Hilfszeile des Setup Tool *OPERATING*, *State of last operation* zeigt *running* an.

  Wenn die Aktion erfolgreich ausgeführt wurde, wird unter *Type of last operation load (FLASH --> MEMORY)* angezeigt, *State of last operation* nimmt den Wert *done* an.

  Die Konfigurationsdatei boot wurde ins Memory von **BinGO!** geladen, die Einstellungen sind aktiv.
- Verlassen Sie ***CONFIGURATION MANAGEMENT*** mit **EXIT**.

  Sie befinden sich wieder im Hauptmenü.

Mit dem Protokoll XMODEM gibt es über die serielle Schnittstelle eine weitere Möglichkeit, Konfigurationsdateien zu transferieren. Die Vorgehensweise wird in der Software Reference dargestellt.

9.2 Software-Update durchführen

Da BinTec Communications AG die Software für alle Produkte ständig weiterentwickelt und Sie sicher die neuen Funktionen von **BinGO!** nutzen wollen, erfahren Sie hier, wie Sie ein Software-Update durchführen können.

www.bintec.de

Wenn Sie ein Software-Update durchführen, spielen Sie auf **BinGO!** ein neues Software-Image (Boot-Image) ein. Jedes Boot-Image beinhaltet neue Funktionen, bessere Performance und bei Bedarf Bugfixes der vorhergehenden Version. Die aktuellen von BinTec Communications AG kostenlos zur Verfügung gestellten Software-Images finden Sie über das World Wide Web unter www.bintec.de. Hier finden Sie auch aktuelle produktspezifische Dokumentation (Release Notes, Handbücher, Kurzanleitungen) und produktübergreifende Dokumentation (Software Reference, Extended Feature Reference, BRICKware for Windows).

Wenn Sie ein Software-Update durchführen, beachten Sie unbedingt die dazugehörige Release Note. Hier sind die Änderungen beschrieben, die mit dem neuen Boot-Image zur Verfügung stehen.

update

Es gibt verschiedene Möglichkeiten, ein Software-Update durchzuführen. In diesem Kapitel erfolgt das Update mit Hilfe des update-Kommandos auf der SNMP-Shell und wird Schritt für Schritt genau beschrieben. Weitere Möglichkeiten finden Sie in der Software Reference und in Kapitel 11.5, Seite 312.

In seltenen Fällen ist zusätzlich ein Update von Bootmonitor und/oder Firmware Logic empfohlen. Falls dies bei einem neuen Release nötig sein sollte, ist dies ausdrücklich in der entsprechenden Release Note vermerkt. Die Vorgehensweise und Empfehlung finden Sie in der Release Note Bootmonitor and Firmware Logic Update.

Soweit BinTec Communications AG keine explizite Empfehlung ausspricht, Bootmonitor oder Firmware Logic upzudaten, sollten Sie dies nicht tun!

ToDo Gehen Sie folgendermaßen vor, um ein Software-Update (Boot-Image) durchzuführen:

Schalten Sie **BinGO!** nicht aus, während das Update durchgeführt wird!

Deaktivieren Sie vor Durchführung des Updates den Autologout mit Eingabe von `t 0` in der SNMP-Shell.

- Geben Sie die URL `www.bintec.de` in Ihren Browser (z. B. Internet Explorer oder Netscape Navigator) ein.

  Die BinTec-Homepage erscheint.

- Klicken Sie auf FTP-Server.

  Dort finden Sie die aktuelle Software und Dokumentation für BinTec-Produkte.

- Klicken Sie auf BinGO!.

  Dort finden Sie die aktuelle Software und Dokumentation für **BinGO!**.

- Klicken Sie mit der rechten Maustaste auf das aktuelle Boot-Image, z. B. Boot-Image Rel. 5.1 Rev.1.

- Klicken Sie im Kontextmenü auf **Save link as...**

- Geben Sie das Verzeichnis und den Namen an, unter dem das neue Boot-Image auf Ihrem Rechner gespeichert werden soll. Als Verzeichnis normalerweise C:\BRICK bei Windows-PCs und /tftpboot bei Unix-Workstations. Als Name können Sie z. B. bgo511.bg übernehmen.

- Bestätigen Sie mit **SAVE**.

  Das Boot-Image wird auf Ihrem Rechner abgespeichert.

- Aktivieren Sie einen TFTP-Server auf Ihrem Rechner.
  Windows-PC: Klicken Sie auf **Programme** ➧ **BRICKware** ➧ **DIME Tools** im Windows-Startmenü, um die **DIME Tools** zu starten (Installation der **DIME Tools**, siehe Kap. Kapitel 3.3, Seite 46). Aktivieren Sie den TFTP-Server.
  Unix-Rechner: Beachten Sie die Hinweise in der Software Reference.

- Loggen Sie sich auf **BinGO!** ein, falls dies noch nicht geschehen ist.

- Schalten Sie mit `t 0` den Autologout aus.

- Geben Sie in der SNMP-Shell `update <IP-Adresse> <Dateiname>` ein.
  `<IP-Adresse>` ist die IP-Adresse des TFTP-Servers, also z. B. die IP-Adresse Ihres Windows-PCs, auf dem der TFTP-Server der DIME Tools läuft und auf dem Sie das neue Boot-Image abgespeichert haben (z. B. 192.168.1.1).
  `<Dateiname>` ist der Name des Boot-Images, das Sie auf Ihrem Rechner abgespeichert haben (z. B. bgo511.bg).

  Die Datei <Dateiname> wird zunächst in den Arbeitsspeicher von **BinGO!** übertragen und überprüft.

  In der SNMP-Shell erscheint: Perform update (y or n)?

- Geben Sie y ein und bestätigen Sie mit der **Eingabetaste**.

  Das Software-Update wird durchgeführt, das neue Boot-Image wird in den Flash-Speicher geladen.

BinGO! benötigt einen zusammenhängenden Block an freiem Arbeitsspeicher, der etwas größer als das neue Software-Image ist. Wenn auf **BinGO!** nicht genügend Arbeitsspeicher zu Verfügung steht, bietet **BinGO!** ein incremental update an, wobei das Image "häppchenweise" direkt und ohne Überprüfung in den Flash-Speicher geladen wird. Gehen Sie folgendermaßen vor:

Wenn zu wenig Arbeitsspeicher verfügbar ist, erscheint in der SNMP-Shell: Do you want to perform an incremental update (y or n)?

- Geben Sie zunächst n ein.
- Geben Sie `update -v <IP-Adresse> <Dateiname>` ein.

  Das Image wird überprüft, noch nicht geladen.
- Geben Sie `update <IP-Adresse> <Dateiname>` ein.

  In der SNMP-Shell erscheint: Perform update (y or n)?
- Geben Sie y ein und bestätigen Sie mit der **Eingabetaste**.

  BinGO! führt ein incremental update aus, das Image wird in den Flash-Speicher geladen. Dieser Vorgang dauert länger als ein normales Update!

  In der SNMP-Shell erscheint: Reboot now (y or n)?
- Geben Sie y ein und bestätigen Sie mit der **Eingabetaste**.

  BinGO! startet mit dem neuen Boot-Image. Die vorhandene Konfiguration wird überschrieben.

10 Troubleshooting

Tips Wenn Sie Probleme mit **BinGO!** haben, helfen Ihnen die folgenden Tips häufig schon weiter:

- Loggen Sie sich auf **BinGO!** ein und geben Sie in der SNMP-Shell ein:
  `debug all`
  Damit werden alle Debugging-Informationen in der SNMP-Shell ausgegeben.
- Überprüfen Sie die von **BinGO!** erzeugten Syslog-Messages (siehe Kapitel 8.1.1, Seite 236). Insbesondere kann es sinnvoll sein, Syslog-Messages an einen externen Host weiterzuleiten und zu speichern, um die Ausgaben eines längeren Zeitraums auswerten zu können.

Zur Interpretation der Debugging-Informationen und Syslog-Messeges siehe Software Reference.

Was die Ursachen für spezielle Probleme sein können und wie Sie dies herausfinden, zeigt Ihnen dieses Kapitel. Es ist folgendermaßen gegliedert:

- Hilfsmittel zum Troubleshooting
- Typische Fehlersituationen

10.1 Hilfsmittel zum Troubleshooting

Hier finden Sie Methoden, um die Ursache Ihres Problems einzugrenzen:

- Lokale SNMP-Shell-Kommandos
- Externe Hilfsmittel

10.1.1 Lokale SNMP-Shell-Kommandos

Diese Kommandos geben Sie direkt in die SNMP-Shell von **BinGO!** ein:

debug

Mit dem Kommando `debug` können Sie die Fehlersuche für eines oder mehrere Subsysteme von **BinGO!** betreiben. Eine genaue Erläuterung der Syntax und der Optionen finden Sie in Kapitel 12.1, Seite 316.

Beispiele:

- Geben Sie `debug all` ein, um Debugging-Informationen für alle Subsysteme anzuzeigen.
- Geben Sie `debug config &` ein, um Problemen beim Konfigurationsmanagement auf die Spur zu kommen (siehe Kapitel 9, Seite 279).

Wenn Sie einem SNMP-Shell-Kommando ein & anhängen, wird das Programm im Hintergrund ausgeführt.

isdnlogin

Mit dem Kommando `isdnlogin` können Sie überprüfen, ob eine ISDN-Verbindung zustande kommen kann. Eine Beschreibung finden Sie in Kapitel 12.1, Seite 316.

Beispiel:

- Geben Sie `isdnlogin 1234 telephony` ein, um ein Telefon mit der Rufnummer 1234 in Ihrem lokalen Büro anzurufen.

  Wenn eine Verbindung zustandekommt, klingelt das Telefon.

trace

Mit dem Kommando `trace` können Sie über ISDN (D- und B-Kanäle) oder über das LAN gesendete und empfangene Datenpakete anzeigen und interpretieren lassen. Eine Beschreibung der Syntax finden Sie in Kapitel 12.1, Seite 316.

Beispiele:

- Geben Sie `trace -ip next` ein, um Datenpakete anzuzeigen, die über den nächsten zu öffnenden B-Kanal laufen.
- Geben Sie `trace -x -s me -d 0:a0:f9:d:5:a 0 0 1` ein, um Datenpakete auszugeben, die von **BinGO!**s MAC-Adresse über das LAN zum Host mit der MAC-Adresse 0:a0:f9:d:5:a verschickt werden.

10.1.2 Externe Hilfsmittel

Mit den folgenden Hilfsprogrammen können Sie von einem Windows-PC oder einem Unix-Rechner aus Verbindungen mit **BinGO!** analysieren.

DIME Tracer (Windows)

Der DIME Tracer ermöglicht, **BinGO!**s ISDN- und CAPI-Datenverkehr von einem Windows-PC aus zu verfolgen. DIME Tracer ist Teil der DIME Tools. Ausführliche Erläuterungen finden Sie in BRICKware for Windows.

bricktrace (Unix)

Das Programm bricktrace ermöglicht, über **BinGO!**s ISDN-Kanäle laufende Daten von einem Unix-Rechner aus zu überprüfen. Bricktrace ist Teil der BRICKtools für UNIX auf Ihrer BinTec Companion CD. Eine ausführliche Beschreibung finden Sie in Kapitel 12.2, Seite 322.

10.2 Typische Fehlersituationen

Im Folgenden finden Sie eine Zusammenstellung typischer Fehlersituationen und Hinweise zu Diagnose und "Heilung". Versuchen Sie, das auftretende Problem einzugrenzen. Folgende Kategorien stehen zur Verfügung:

- System-Fehler
- ISDN-Verbindungen
- IPX-Routing

10.2.1 System-Fehler

Ich habe mein Paßwort vergessen.

Sie müssen **BinGO!** in den unkonfigurierten Anfangszustand (Auslieferungszustand) zurückversetzen, wie er ausgeliefert wurde:

- Verbinden Sie Ihren Rechner über die serielle Schnittstelle mit **BinGO!** wie in Kapitel 5.1.3, Seite 106 beschrieben.
- Schalten Sie **BinGO!** aus und wieder ein.

  Sie sehen diverse Selbsttests und dann "Press <sp> for boot monitor or any other key to boot system".
- Drücken Sie nun die Leertaste.

  Ein BOOTmonitor-Menü wird angezeigt.
- Wählen Sie (4) Delete Configuration und bestätigen Sie mit der **Eingabetaste**. Beachten und bestätigen Sie die nachfolgenden Sicherheitsabfragen.

  Sowohl das Paßwort als auch die komplette Konfiguration von **BinGO!** werden gelöscht.
- Wählen Sie (1) Boot System.

  BinGO! wird neu gestartet.
- Konfigurieren Sie **BinGO!** erneut.

Ich kann BinGO! im LAN nicht erreichen.

Versuchen Sie eine serielle Verbindung herzustellen:

- Verbinden Sie Ihren Rechner über die serielle Schnittstelle mit **BinGO!**.
- Loggen Sie sich als Benutzer `admin` mit dem entsprechenden Paßwort ein.
- Starten Sie das Setup-Tool mit `setup`.
- Untersuchen Sie, ob ein Konfigurationsfehler die Ursache ist: Haben Sie unter ***CM-BNC/TP, ETHERNET*** die IP-Adresse eingetragen? Haben Sie unter ***IP*** ➧ ***ACCESS LISTS*** ein Filter eingetragen, das Sie aussperrt? Machen Sie die erforderlichen Korrekturen.

Wenn auch eine serielle Verbindung nicht klappt:

- Überprüfen Sie die Einstellungen des Terminal-Programms (siehe Kapitel 5.1.1, Seite 103). Wenn Sie die Standard-Einstellungen im BOOTmonitor verändert haben, passen Sie Ihre Terminaleinstellungen daran an.
- Wenn Sie keinen Erfolg haben, gehen Sie vor wie unter "Ich habe mein Paßwort vergessen" beschrieben.

10.2.2 ISDN-Verbindungen

Hier finden Sie mögliche Fehlerquellen für ISDN-Verbindungen.

Die Telefonrechnung ist ungewöhnlich hoch.

Nutzen Sie die Funktion Taschengeldkonto (siehe Kapitel 7.1.3, Seite 196). Damit können Sie für Verbindungen mit **BinGO!** ein Limit festlegen, um Gebühren aufgrund von Fehlern bei der Konfiguration in Grenzen zu halten.

Möglicherweise gibt es auf **BinGO!** ISDN-Verbindungen, die ständig offen bleiben oder es werden ungewollte ISDN-Verbindungen provoziert.

- Überprüfen Sie mit `debug all` oder `trace`, ob ein Rechner im LAN eine andere Netzmaske verwendet als auf **BinGO!** eingetragen ist.

- Überprüfen Sie mit `debug all` oder `trace`, ob ein Rechner im LAN mit einer falschen IP-Adresse für Remote-CAPI konfiguriert ist (Zielport 2662).
- Überprüfen Sie in ***SYSTEM*** ➧ ***EXTERNAL SYSTEM LOGGING***, ob **BinGO!** so konfiguriert ist, daß Syslog-Messages auf einen Host außerhalb des LANs geschickt werden (Zielport 514).
- Überprüfen Sie in der MIB-Tabelle **biboAdmTrapHostTable**, ob **BinGO!** so konfiguriert ist, daß SNMP-Traps auf einen Host außerhalb des LANs geschickt werden (Zielports 161, 162).
- Überprüfen Sie, ob bei Verbindungen mit dynamischem Channel Bundling häufiges Auf- und Abbauen des zweiten B-Kanals aufgrund von schwankendem Traffic geschieht.
- Überprüfen Sie mit `debug all` oder `trace`, ob ein Rechner im LAN mit einer falschen IP-Adresse für den WINS-Server konfiguriert ist (Zielports 137-139). Konfigurieren Sie gegebenenfalls den Rechner richtig oder setzen Sie entsprechende Filter ein.
- Überprüfen Sie mit `debug all` oder `trace`, ob ein Rechner im LAN für Namensauflösung von NetBIOS-Namen mit Hilfe von DNS konfiguriert ist (es wird von einem Clientport aus auf Zielport 53 zugegriffen). Versuchen Sie nicht, NetBIOS-Namen mit DNS aufzulösen!
- Überprüfen Sie mit `debug all` oder `trace`, ob eine Applikation auf einem Rechner im LAN versucht, Adressen aufzulösen, die der Name-Server beim Internet Service Provider nicht kennt (es wird von einem Clientport aus auf Zielport 53 zugegriffen). Richten Sie eine lokale HOSTS-Datei im Windows-Verzeichnis ein, die die Namensauflösung durchführen kann (siehe Kapitel 4.5, Seite 91).
- Überprüfen Sie mit `debug all` oder `trace`, ob auf einem Rechner im LAN NetBIOS over IP eingerichtet ist (es wird vom Sourceport 137 auf den Zielport 53 zugegriffen). Dabei wird versucht, NetBios-Namen über DNS aufzulösen. Schalten Sie NetBIOS over IP ab oder setzen Sie Filter ein (Konfiguration der entsprechenden Filter finden Sie in Kapitel 6.1.6, Seite 145 oder nutzen Sie den einfachen NetBIOS-Filter des Configuration Wizards, siehe Kapitel 3.4.1, Seite 51).
- Überprüfen Sie, ob Sie Callback konfiguriert haben (siehe Kapitel 8.2.4, Seite 250) und dabei eine falsche Rufnummer eingegeben haben (*Number* unter ***WAN PARTNER*** ➧ ***EDIT*** ➧ ***WAN NUMBERS*** ➧ ***EDIT***).

- Überprüfen Sie, ob Sie ein trace-Programm über eine ISDN-PPP-Verbindung laufen lassen. Damit werden ständig Pakete über die ISDN-Verbindung gesendet, die Verbindung bleibt permanent offen.

Ausgehende Rufe kommen nicht zustande.

- Überprüfen Sie anhand der LEDs auf der **BinGO!**-Vorderseite (siehe Kapitel 11.2, Seite 305), ob eine Verbindung zustande kommt.
- Überprüfen Sie mit `isdnlogin`, ob ausgehende Rufe möglich sind.
- Überprüfen Sie in ***Monitoring and Debugging*** ➧ ***ISDN Monitor***, ob überhaupt ein ausgehender Ruf protokolliert wurde, ob die gewählte Nummer korrekt ist und ob der Ruf verbunden war.
- Überprüfen Sie, ob ISDN-Syslog-Messages mit "disconnect cause" protokolliert wurden.
- Überprüfen Sie, ob *Encapsulation* in ***WAN Partner*** ➧ ***Edit*** für die Verbindungspartner identisch ist.
- Überprüfen Sie, ob *Authentication* in ***WAN Partner*** ➧ ***Edit*** ➧ ***PPP*** für die Verbindungspartner identisch ist.
- Überprüfen Sie mit `trace`, was über die ISDN-Kanäle gesendet wird.
- Überprüfen Sie, ob die MIB-Variable **Status** in der MIB-Tabelle **isdnStkTable** den Wert *loaded* hat.
- Überprüfen Sie, ob in ***CM-1BRI, ISDN S0*** ➧ ***Incoming Call Answering*** die eigene Rufnummer richtig eingetragen ist. Sie gilt auch für ausgehende Rufe!

Eingehende Rufe kommen nicht zustande.

- Überprüfen Sie anhand der LEDs auf der **BinGO!**-Vorderseite (siehe Kapitel 11.2, Seite 305), ob ein eingehender Ruf überhaupt empfangen wird.
- Überprüfen Sie in ***Monitoring and Debugging*** ➧ ***ISDN Monitor***, ob überhaupt ein eingehender Ruf protokolliert wurde.
- Überprüfen Sie in ***WAN Partner*** ➧ ***Edit*** ➧ ***WAN Numbers***, ob eine passende Nummer für eingehende Rufe eingetragen ist.

- Überprüfen Sie die MIB-Variablen **DSS1Cause**, **1TR6Cause** und **Local-Cause** in der MIB-Tabelle **isdnCallHistoryTable**. Zur Interpretation der Einträge siehe Software Reference.
- Überprüfen Sie in ***CM-1BRI, ISDN S0*** ➧ ***INCOMING CALL ANSWERING,*** ob Sie für eingehende Rufe die erforderlichen Eintragungen gemacht haben.
- Überprüfen Sie, ob *Encapsulation* in ***WAN PARTNER*** ➧ ***EDIT*** für die Verbindungspartner identisch ist.
- Überprüfen Sie, ob *Authentication* in ***WAN PARTNER*** ➧ ***EDIT*** ➧ ***PPP*** für die Verbindungspartner identisch ist.

10.2.3 IPX-Routing

Hier finden Sie einige Probleme mit dazugehörigen Lösungsvorschlägen, die bei IPX-Routing auftreten könnten.

Überprüfen Sie mit dem Setup Tool:

- Haben Sie unter ***LICENSES*** die richtige Lizenz eingetragen?
- Ist in ***IPX*** der Eintrag unter *Internal Network Number* eindeutig im LAN?

Ein Server existiert in einem Remote-LAN (LAN-LAN-Kopplung über ISDN), aber ist für Clients im lokalen LAN "unsichtbar".

Der Server könnte für Clients unsichtbar sein, weil SAP-Pakete vom Server nicht empfangen werden:

- Überprüfen Sie die Eintragungen von *Update Time* und *Age Multiplier* in ***WAN PARTNER*** ➧ ***EDIT*** ➧ ***IPX***. Die Einstellungen müssen zu den Einstellungen auf den Servern im **BinGO!**-LAN kompatibel sein.
- Überprüfen Sie, ob ein dazwischenliegender Router die SAP-Pakete ausfiltert.
- Überprüfen Sie mit isdnlogin, ob eine ISDN-Verbindung zwischen Client und Server zustande kommen kann.
- Überprüfen Sie, ob Sie unter ***CM-BNC/TP, ETHERNET*** *local IPX-NetNumber* und *Encapsulation* richtig eingetragen haben und ob der Server sie empfangen kann.

Wenn der Client versucht, einen Server in einem Remote-Netzwerk über eine PPP-Verbindung zu erreichen, wartet er sehr lange und die Verbindung wird evtl. abgebrochen.

In manchen Fällen meldet der lokale Router dem Client fälschlicherweise, daß ein Server erreichbar ist.

- Überprüfen Sie, ob der Server abgestürzt und das Aging-Intervall noch nicht abgelaufen ist. Verändern Sie gegebenenfalls die Einstellung von *Send RIP/SAP Updates* unter ***WAN PARTNER*** ➧ ***EDIT*** ➧ ***IPX***.
- Überprüfen Sie, ob der Server und der Router im Remote-Netzwerk gleichzeitig inaktiv sind (z. B. wegen Stromausfall). Setzen Sie die WAN-Schnittstelle des entsprechenden WAN-Partners mit dem Befehl `ifconfig` kurz auf *down* und anschließend wieder auf *dialup*, um die vom WAN-Partner gelernten Routen und Dienste zu löschen.

Ich kann auf dem Client nicht auf ein Netz-Laufwerk des Clients wechseln.

- Möglicherweise ist der Server für den Client unsichtbar. Gehen Sie vor wie unter "Ein Server existiert in einem Remote-LAN ..." beschrieben.
- Überprüfen Sie, ob die auf dem Server zur Verfügung stehenden Lizenzen alle belegt sind.

ISDN-Verbindungen werden ständig neu aufgebaut.

Es sind nicht nur RIP/SAP-Pakete, die den Aufbau von ISDN-Verbindungen verursachen.

- Überprüfen Sie, ob sich ein Eintrag in der MIB-Tabelle **ipxDenyTable** befindet, der verhindert, daß Novell Serialization-Pakete über die Wählverbindung gesendet werden.
- Überprüfen Sie, ob Sie unter ***IPX*** *enable IPX spoofing* und *enable SPX spoofing* mit *yes* aktiviert haben.
- Überprüfen Sie, ob irgendwo RCONSOLE mit einem ständig sich verändernden Bildschirm (z. B. MONITOR, IPXCON, TCPCON, ein Bildschirmschoner, usw.) aktiv ist.

- Überprüfen Sie, ob im LAN NetBIOS over IPX verwendet wird (Windows for Workgroups, NT, Win95). Wählen Sie gegebenenfalls unter ***IPX*** für *NetBIOS Broadcast replication no* oder *on LAN only* aus.
- Überprüfen Sie, ob NDS Replica Synchronization aktiv ist (ab Netware 4.1 Server).
- Werten Sie die Syslog-Messages (*Level* = *debug*) aus und filtern Sie gegebenenfalls die IPX-Pakete aus, die dort als Ursache für ungewollte Verbindungsaufbauten genannt werden.

Die MIB-Variable ipxAdmSpxConns enthält mehr Verbindungen als tatsächlich aktiv sind.

BinGO! empfängt möglicherweise keine SPX-Abbruch-Meldungen vom Server:

- Geben Sie das Kommando `reset router` an der Konsole des entsprechenden Servers ein.

  Alle inaktiven Verbindungen zwischen dem Server und **BinGO!** werden abgebaut.
- Bei fehlender Abmeldung könnten SPX-Verbindungen noch bis zu einem Timeout bestehen und dadurch in **ipxAdmSpxConns** mitgezählt werden.

11 Technische Daten

In diesem Kapitel werden die technischen Daten von **BinGO!** vorgestellt. Folgende Bereiche werden behandelt:

- Allgemeine Produktmerkmale
- **BinGO!**-Vorderseite mit den Anzeigen (LEDs)
- **BinGO!**-Rückseite mit den Anschlüssen
- Pin-Zuordnung
- BOOTmonitor

11.1 Allgemeine Produktmerkmale

Die allgemeinen Produktmerkmale umfassen die Leistungsmerkmale von **BinGO!** und technische Voraussetzungen für Installation und Betrieb.

Bezeichnung	Werte
Produktname:	**BinGO!**
Geschlecht:	männlich :-)
Maße und Gewichte (B x H x T): Gerätemaße ohne Kabel Aufstellgröße und Wartungsfläche Gewicht Transportgewicht (inkl. Dokumentation, Kabel, Verpackung)	 141 mm x 50 mm x 145 mm 150 mm x 60 mm x 210 mm 420 g 2 kg
Speicher:	4 MB / 32 bit DRAM, 1 MB / 8 bit flash-ROM
LEDs:	6 (1 Power, 4 Funktion, 1 Error)
Leistungsaufnahme Gerät:	2 W (typisch)
Spannungsversorgung:	AC/DC-Adapter Eingang: 230V~50Hz / 70mA Ausgang: 5V-800mA 4VA
Umweltanforderungen: Lagertemperatur Betriebstemperatur Relative Luftfeuchtigkeit Raumklassifizierung	 -20 - +85˚C 0 - 50˚C 20 - 90% nichtkondensierend im Betrieb. 5 - 95% nichtkondensierend bei Lagerung. Nur in trockenen Räumen betreiben.
MTBF-Wert:	100 000 Stunden

Bezeichnung	Werte
Verfügbare Interfaces:	
Serielle Schnittstelle V.24	Fest eingebaut, unterstützt die Baudraten: 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200 Baud.
Ethernet IEEE802.3 LAN	Fest eingebaut (nur twisted-pair), node/hub-switch.
ISDN-WAN S_0	Fest eingebaut.
Verwendete Stecker:	
serielle Schnittstelle Ethernet-Schnittstelle ISDN-Schnittstelle	Sub-D 9 male (DTE) RJ45 RJ45
Applikations-Schnittstelle:	Dual-Remote-CAPI (v1.1 und 2.0), R-CAPI-Treiber für Windows 3.11/95/NT und Novell Netware. Source Code Library für andere Systeme (z. B. Unix, AS400).
Datenkompression:	PPP LZS STAC Kompressionsrate bis 4:1.
SAFERNET™ Security Technologie:	Community Paßworte, PAP, CHAP, MS-CHAP, Callback, Access Control Lists, Allow Lists, CLID, RADIUS, NAT, TAF, MPPE Encryption.
Erforderliche Lizenzen:	Lizenzen für CAPI, IP, IPX, STAC im Lieferumfang enthalten. Zusatzlizenzen für VPN und unbegrenzte Anzahl an LAN-Nutzern erhältlich.
Mitgelieferte Software:	RVS-COM Lite (Kommunikationsanwendung) BRICKware for Windows BRICKtools for Unix

Bezeichnung	Werte
Mitgelieferte gedruckte Dokumentation:	User's Guide (engl.) Kurzanleitung (dt.) Quick Install Guide (engl.)
Online-Dokumentation:	BRICKware for Windows (engl.) Software Reference (engl.) Extended Feature Reference (engl.) User's Guide (dt.)

11.2 LEDs auf der Vorderseite

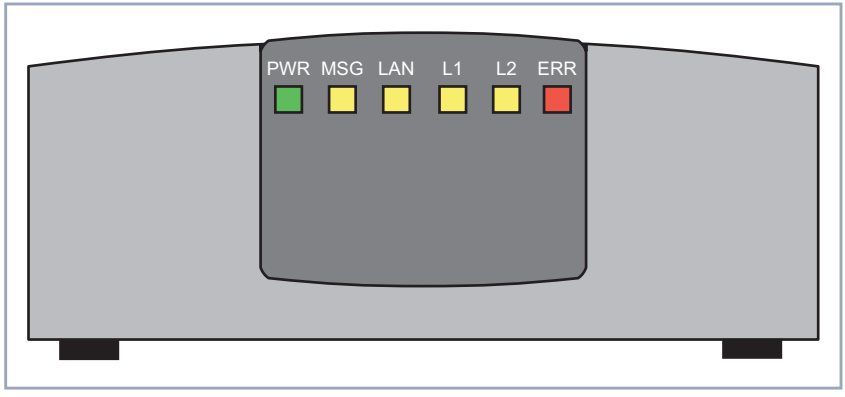


Bild 11-1: **BinGO!** Vorderseite

Auf der Vorderseite befinden sich sechs Anzeigen (LEDs), die Statusinformationen von **BinGO!** anzeigen. Jede der LEDs ist mit mehreren Bedeutungen belegt, je nachdem in welchem Modus **BinGO!** sich befindet. Wenn **BinGO!** hochfährt, wechseln die verschiedenen Funktionszustände zwischen:

- Start-Modus
- BOOTmonitor-Modus (siehe Kapitel 11.5, Seite 312)
- Normaler Betriebs-Modus

Die Bedeutungen der LEDs im jeweiligen Zustand sind in den folgenden Tabellen beschrieben.

Start-Modus

LED	Status	Bedeutung
PWR	An	Stromversorgung ist angeschlossen.
MSG	Blinkend	DRAM-Test wird durchgeführt.
LAN	Aus	Wird nicht genutzt.
L1	Blinkend	Flash ROM-Test wird durchgeführt.
L2	Blinkend	CHIP-Test wird durchgeführt.
ERR	Aus	Wird nicht genutzt.

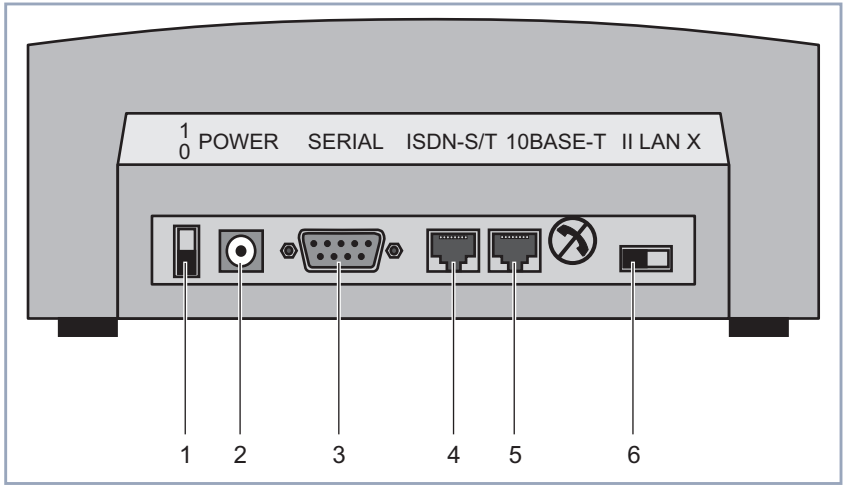
BOOTmonitor-Modus

LED	Status	Bedeutung
PWR	An	Stromversorgung ist angeschlossen.
MSG	Aus	Wird nicht genutzt.
LAN	Blinkend	TFTP-Transfer wird durchgeführt.
L1, L2, ERR	An	BOOTmonitor ist aktiv (oder erwartet eine Eingabe über die Tastatur).
L1, L2, ERR	Blinkend	BOOTmonitor dekomprimiert Boot-Image.

Normaler Betriebs-Modus

LED	Status	Bedeutung
PWR	An	Stromversorgung ist angeschlossen.
MSG	–	Reserviert für zukünftige Anwendung.
LAN	An	Datenpaket passiert die LAN-Schnittstelle.
L1, L2	An	Datenverkehr über ISDN-B-Kanal 1 bzw. 2.
ERR	An (zeitweilig)	Kollision im LAN wurde erkannt (jedes Aufleuchten zeigt eine Kollision an).
ERR	An (konstant)	Die LAN-Verbindung wurde nicht hergestellt (kein 10Base-T-Kabel angeschlossen) oder der LAN-Schalter befindet sich in der falschen Position.

11.3 Anschlüsse auf der Rückseite



1	Ein-/Ausschalter	4	S_0-Schnittstelle (ISDN)
2	Stromversorgungsanschluß	5	10Base-T-Schnittstelle (LAN)
3	Serielle Schnittstelle	6	LAN-Schalter

Bild 11-2: **BinGO!** Rückseite

Die **BinGO!**-Hauptplatine enthält eine LAN- und eine ISDN-Schnittstelle. Diese Schnittstellen sind über die an der Rückseite angebrachten Anschlüsse (Kapitel 11.4, Seite 308) zu erreichen.

Achtung!

Die Verwendung eines falschen Netzadapters kann zum Defekt Ihres Routers führen!

- Verwenden Sie ausschließlich das mitgelieferte Steckernetzteil (5 V DC).
- Vergewissern Sie sich, daß die auf dem Steckernetzteil vermerkte Nennspannung mit der lokalen Spannungsversorgung übereinstimmt.
- Tauschen Sie niemals die Netzadapter von **BinGO!** und **BinGO! Plus/Professional** aus.

11.4 Pin-Zuordnung

Serielle Schnittstelle:

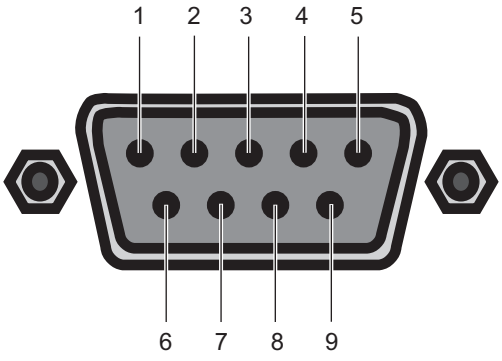


Bild 11-3: 9-polige Sub-D-Buchse

Als Konsolenanschluß stellt **BinGO!** eine serielle Schnittstelle mit 9-poliger Sub-D-Buchse. Baudraten zwischen 1200 und 115200 werden unterstützt. Die Pin-Zuordnung wurde modifiziert, um für eine größere Auswahl an Terminals kompatibel zu sein.

Die Pin-Zuordnung für die 9-polige Sub-D-Buchse (3) ist wie folgt:

Pin	Funktion
1	DCD (nicht verbunden)
2	Empfangen
3	Senden
4	DTR - DSR (umgeleitet zu Pin 6)
5	GND
6	DSR - DTR (umgeleitet zu Pin 4)
7	RTS - CTS (umgeleitet zu Pin 8)
8	CTS - RTS (umgeleitet zu Pin 7)
9	Nicht verbunden

ISDN-S_0-Schnittstelle

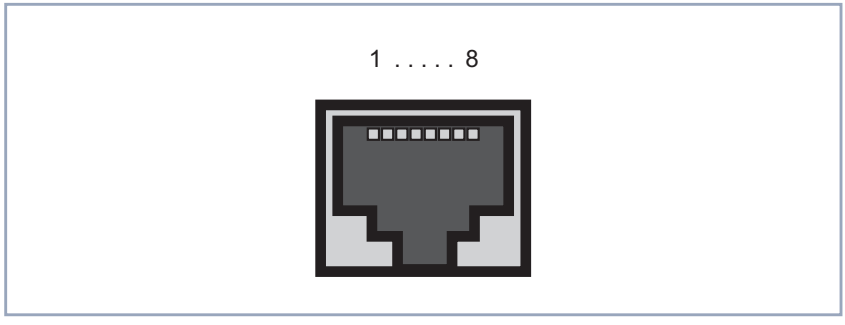


Bild 11-4: ISDN-S_0-BRI-Schnittstelle (RJ45-Buchse)

Die Pin-Zuordnung für die ISDN-S0-BRI-Schnittstelle (RJ45-Buchse) (4) ist wie folgt:

Pin	Funktion
1	Nicht genutzt
2	Nicht genutzt
3	Senden (+)
4	Empfangen (+)
5	Empfangen (-)
6	Senden (-)
7	Nicht genutzt
8	Nicht genutzt

LAN-Schnittstelle

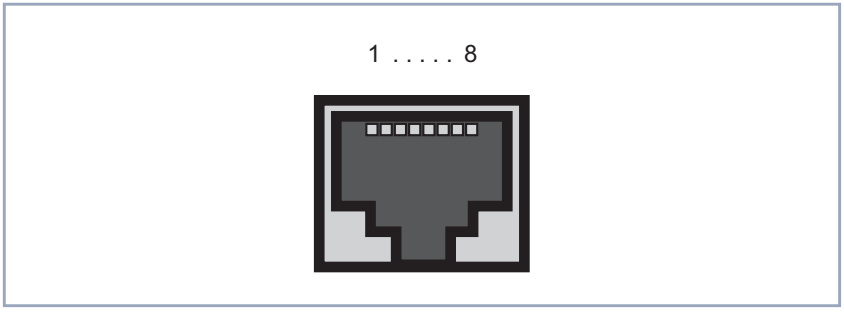


Bild 11-5: Ethernet 10Base-T-Schnittstelle (RJ45-Buchse)

Die Pin-Zuordnung für die Ethernet 10Base-T-Schnittstelle (RJ45-Buchse) ist wie folgt:

Pin	Funktion
1	TD +
2	TD -
3	RD +
4	Nicht genutzt
5	Nicht genutzt
6	RD -
7	Nicht genutzt
8	Nicht genutzt

Wenn Sie die LAN-Schnittstelle von **BinGO!** nicht an einen externen Hub, sondern direkt an der Ethernet-Karte Ihres Rechners anschließen wollen, müssen Sie den LAN-Schalter (6) auf der Geräterückseite auf ⤫ stellen. Mit dieser Einstellung können Sie das mitgelieferte 1 zu 1 verdrahtete LAN-Kabel verwenden und brauchen kein Crossover-Kabel.

11.5 BOOT-Sequenz

Beim Hochfahren von **BinGO!** werden verschiedenen Funktionszustände durchlaufen (siehe auch Kapitel 11.2, Seite 305):

- Start-Modus
- BOOTmonitor-Modus
- Normaler Betriebs-Modus

Nachdem im Start-Modus einige Selbsttests erfolgreich ausgeführt wurden, erreicht **BinGO!** den BOOTmonitor-Modus. Der BOOTmonitor-Prompt wird angezeigt, falls Sie über ein Terminalprogramm mit **BinGO!** verbunden sind.

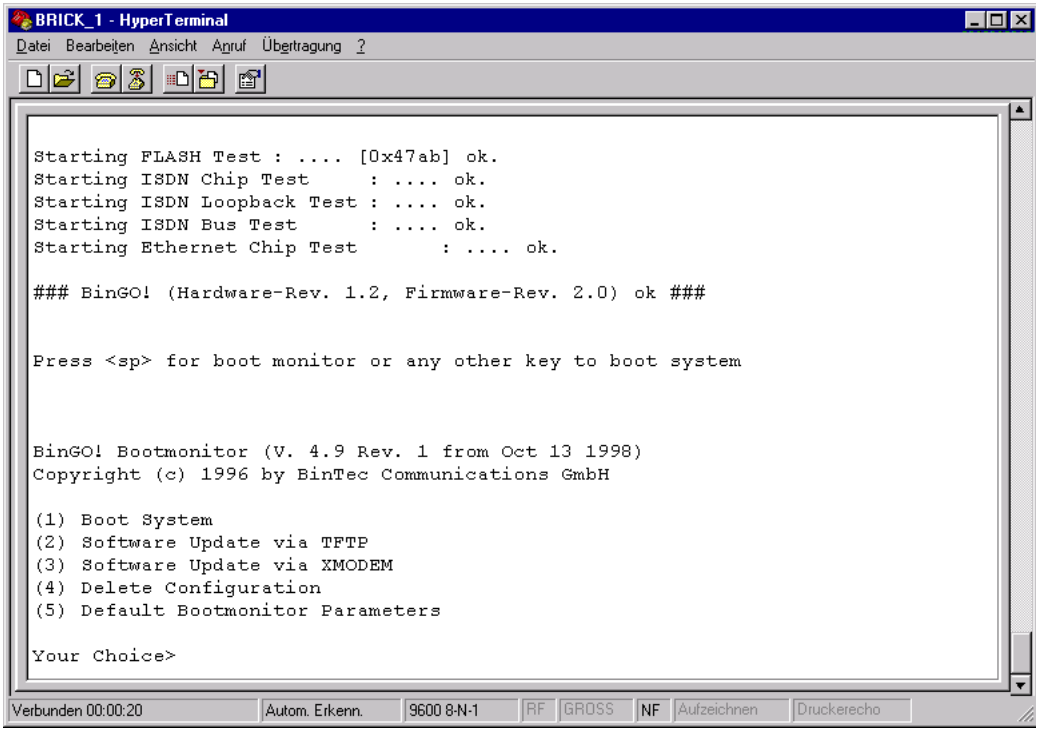


Bild 11-6: BOOTmonitor

BOOTmonitor Betätigen Sie nach Anzeige des BOOTmonitor-Prompts (Bild 11-6, Seite 312) innerhalb von 4 Sekunden die **Leertaste**, um die Funktionen des BOOTmonitors zu nutzen. Wenn Sie keine Eingabe machen, wechselt **BinGO!** nach Ablauf der 4 Sekunden in den normalen Betriebs-Modus.

Funktionen Folgende Funktionen stellt der BOOTmonitor zur Verfügung, die Sie durch Eingabe der entsprechenden Ziffer auswählen (für detaillierte Informationen beachten Sie bitte die Software Reference):

- (1) Boot System:
  BinGO! lädt die komprimierte Boot-Datei vom Flash-Speicher in den Arbeitsspeicher. Dies wird beim Hochfahren automatisch ausgeführt.
- (2) Software Update via TFTP:
  BinGO! führt ein Software-Update über einen TFTP-Server aus.
- (3) Software Update via XMODEM:
  BinGO! führt ein Software-Update über eine serielle Schnittstelle mit XMODEM aus.
- (4) Delete Configuration:
  BinGO! wird in den Auslieferungszustand zurückversetzt. Alle Konfigurationsdateien werden gelöscht, die BOOTmonitor-Einstellungen werden auf die Standardwerte gesetzt.
- (5) Default BOOTmonitor Parameters:
  Sie können die Standard-Einstellungen von **BinGO!**s BOOTmonitor verändern, z. B. die Baudrate für serielle Verbindungen.

Wenn Sie die Baudrate verändern (voreingestellt ist 9600 Baud), achten Sie darauf, daß das verwendete Terminalprogramm diese Baudrate verwendet. Wenn dies nicht der Fall ist, können Sie keine serielle Verbindung zu **BinGO!** herstellen!

11 Technische Daten

12 Wichtige Kommandos

Dieses Kapitel beschreibt folgende Kommandos:

- SNMP-Shell Kommandos:
  - telnet
  - ping
  - trace
  - isdnlogin
  - debug
  - ifconfig
  - ifstat
  - netstat
  - date
  - t
- BRICKtools for Unix Kommandos:
  - bricktrace
  - capitrace

12.1 SNMP-Shell-Kommandos

Auf **BinGO!** sind einige Programme vorinstalliert, die direkt von der SNMP-Shell aus gestartet werden können. Eine kurze Beschreibung der gebräuchlichsten Programme und die dazugehörige Kommandozeile, die Sie zum Starten der jeweiligen Programme in der SNMP-Shell eingeben, folgen:

Bitte beachten Sie:
Parameter der Kommandozeile in eckigen Klammern [] stellen optionale Werte dar. Begriffe in spitzen Klammern <> können mehrere Werte annehmen. Geben Sie keine Klammern ein!

telnet

```
telnet [-f] <host> [<port>]
```

Wird benutzt, um mit einem anderen Host zu kommunizieren.

- `-f`: Legt fest, daß die telnet-Sitzung transparent sein soll. Diese Option ist vor allem für Verbindungen mit nicht-telnet-Ports (z. B. uucp oder smtp) nützlich.
- `host`: IP-Adresse oder Name des Hosts.
- `port`: Port-Nummer.

ping

```
ping [-c <count>] <host> [<size>]
```

Wird benutzt, um die Kommunikation mit einem anderen Host zu testen.

- `-c <count>`: Limitiert die Anzahl der gesendeten Pakete, `count` Pakete werden gesendet.
- `host`: IP-Adresse oder Name des Hosts, zu dem echo_request-Pakete gesendet werden.
- `size`: Legt die Größe der gesendeten Pakete fest.

Wenn Sie `-c <count>` nicht angeben, werden so lange Pakete an den Host geschickt, bis Sie den Vorgang abbrechen, z. B. mit `Ctrl-C`.

trace

Für WAN-Schnittstellen:
`trace [-h23aFAtpiNxX] [next] [-T <tei>] [-c <cref>] <channel> <unit> <slot>`

Für LAN-Schnittstellen:
`trace [-h23iNxX1] [-d <destination MAC filter>] [-o] [-s <source MAC filter>]0 0 <slot>`

Wird benutzt, um über ISDN (D- und B-Kanäle) oder über das LAN gesendete und empfangene Datenpakete anzuzeigen und interpretieren zu lassen.

- `-h`: Hexadezimale Ausgabe.
- `-2`: Schicht-2-Ausgabe.
- `-3`: Schicht-3-Ausgabe.
- `-a`: Asynchronous HDLC (nur B-Kanal).
- `-F`: FAX (nur B-Kanal).
- `-A`: FAX und AT-Kommandos (nur B-Kanal).
- `-t`: Ausgabe in ASCII-Text (nur B-Kanal).
- `-p`: PPP (nur B-Kanal).
- `-i`: IP-Ausgabe (nur B-Kanal).
- `-N`: Novell IPX-Ausgabe (nur B-Kanal).
- `-x`: Raw dump mode.
- `-X`: Asynchronous PPP over X.75 (nur B-Kanal).
- `next`: Nur Informationen über den als nächstes geöffneten B-Kanal anzeigen.
- `-T <tei>`: TEI-Filter setzen (nur D-Kanal).
- `-c <cref>`: Callref-Filter setzen (nur D-Kanal).
- `channel`: 0 = D-Kanal oder X.21-Schnittstelle, 1 ... 31 = Bx-Kanal.
- `unit`: 0 ... 1. Selektieren des physikalischen Interface für Module mit zwei Interfaces (z. B. CM-2BRI).
- `slot`: 1 ... 2. Angabe des Slot, in dem das Modul installiert ist.
- `-d <destination MAC filter>`: Definiert Filter für Ziel-MAC-Adresse (nur LAN).
- `-s <source MAC filter>`: Definiert Filter für Quell-MAC-Adresse (nur LAN).

- `-o`: Kombiniert zwei oder mehr -d- oder -s-Filter mit einer logischen ODER-Verknüpfung.
- `MAC filter`: `me` = **BinGO!**'s MAC-Adresse, `bc` = Broadcast-Pakete.

Sie können einen -d-MAC-Filter und einen -s-MAC-Filter mit einer logischen UND-Verknüpfung kombinieren, indem Sie einfach beide definieren.

Um zwei oder mehr -d- und -s-MAC-Filter mit einer logischen ODER-Verknüpfung zu kombinieren, definieren Sie die Filter und trennen Sie mit `-o`.

isdnlogin

```
isdnlogin [-c <stknumber>] [-C] [-s <service>]
[-a <addinfo>] [-b <bits>] isdn-number [isdn-service]|
layer1-protocol]
```

Wird benutzt, um über ISDN eine Remote-Login-Shell auf **BinGO!** zu öffnen.

- `-c <stknumber>`: Auswahl der ISDN-Stacks für diesen Login.
- `-C`: Versucht, Komprimierung (V.42bis) anzuwenden.
- `-s <service>`: 1RT6-Dienst für ausgehende Verbindungen.
- `-a <addinfo>`: Zusätzlicher 1TR6 Info-Code für ausgehende Verbindungen.
- `-b <bits>`: Nur <bits> bits für Übertragung verwenden (Geben Sie z. B. `-b 7` für 7bit ASCII-Übertragung ein).
- `isdn-number`: Rufnummer des ISDN-Partners, bei dem Sie sich einloggen möchten.
- `isdn-service`: Zu verwendender ISDN-Dienst (data, telephony, faxg3, faxg4, btx).
- `layer1-protocol`: Mögliche Werte: v110_1200, v110_2400, v110_4800, v110_9600, v110_19200, v110_38400, modem, dovb56k, telephony.

debug

```
debug [show]|[[-t] all|acct|system|<subs> [<subs> ...]]
```

Wird benutzt, um ausgewählte Debugging-Informationen von **BinGO!**s Subsystemen anzuzeigen.

- `show`: Alle möglichen Subsysteme anzeigen, die auf Fehler untersucht werden können.
- `-t`: Zeitstempel vor jede Debugging-Meldung anhängen.
- `all`: Debugging-Informationen für alle Subsysteme anzeigen.
- `acct`: Debugging-Informationen für das Accounting-Subsystem anzeigen.
- `system`: Debugging-Informationen für alle Subsysteme außer das Accounting-Subsystem anzeigen.
- `subs`: Subsystem, für das Debugging-Informationen angezeigt werden sollen. Mehrere Eingaben sind möglich (getrennt durch ein Leerzeichen).

ifconfig

```
ifconfig <interface> [destination <destaddrs>] [<address>]
[netmask <mask>] [up | down | dialup] [-] [metric <n>]
```

Wird benutzt, um Schnittstellen zum Netzwerk Adressen zuzuweisen und/oder Parameter der Schnittstellen zu konfigurieren und die entsprechenden Einträge in der Routing-Tabelle zu verändern.

Wenn Sie lediglich `ifconfig <interface>` eingeben, werden die aktuellen Parameter von interface angezeigt.

- `interface`: Name der Schnittstelle (**ifDescr**).
- `destination <destaddrs>`: Ziel-IP-Adresse eines Hosts. Damit wird eine Host-Route zu diesem Host in die Routing-Tabelle hinzugefügt (**ipRouteDest**).
- `address`: **BinGO!**s IP-Adresse für die Schnittstelle (**ipRouteNextHop**).
- `netmask <mask>`: Netzmaske der Schnittstelle (**ipRouteMask**).
- `up`: Setzt die Schnittstelle auf den Status up.
- `down`: Setzt die Schnittstelle auf den Status down.
- `dialup`: Setzt die Schnittstelle auf den Status dialup.
- `-`: Definiert keine eigene IP-Adresse (**ipRouteNextHop** = *0.0.0.0*).
- `metric <n>`: Setzt Metrik der Route auf n (**ipRouteMetric1**).

ifstat

```
ifstat [-lur] [<ifcname>]
```

Wird benutzt, um Statusinformationen über die Schnittstellen des Systems anzuzeigen (basierend auf den Eintragungen in der MIB-Tabelle **ifTable**).

- `-l`: Zeigt Informationen der Schnittstelle in voller Länge an (normalerweise wird die Beschreibung nur bis zum 12. Zeichen angezeigt).
- `-u`: Zeigt nur Informationen über die Schnittstellen an, die den Status up haben.
- `-r`: Zeigt die Filter an, die für die Schnittstelle definiert sind.
- `ifcname`: Zeigt nur Informationen zu den Schnittstellen an, deren Namen mit den eingegebenen Zeichen beginnen (z. B. `ifstat en1` zeigt Informationen zu den Schnittstellen en1, en1-IIc und en1-snap an).

netstat

```
netstat [[-i | -r | -p [<interface>]] | -d <dest. IP addr.>]
```

Wird benutzt, um eine kurze Liste an Systeminformationen anzuzeigen.

- `-i`: Zeigt eine Liste der Schnittstellen an.
- `-r`: Zeigt eine Liste der Einträge in der Routing-Tabelle an.
- `-p`: Zeigt eine Liste der WAN-Partner an.
- `interface`: Damit werden die angezeigten Informationen auf die ausgewählte Schnittstelle beschränkt.
- `-d <dest. IP addr.>`: Zeigt Routen zu der angegebenen IP-Adresse an.

date

```
date [YYMMDDHHMMSS]
```

BinGO! hat eine Software-Uhr. Mit Eingabe von `date` wird die eingestellte Uhrzeit angezeigt.

Mit Eingabe von `date YYMMDDHHMMSS` stellen Sie die Uhr auf den entsprechenden Wert ein (Jahr, Monat, Tag, Stunde, Minute, Sekunde).

t

`t [<seconds>]`

Wird benutzt, um den Zeitraum für Autologout für die aktuelle Login-Session zu definieren (standardmäßig wird eine Verbindung zu **BinGO!** über telnet, isdnlogin oder seriell automatisch getrennt, wenn 15 Minuten lang keine Eingabe über die Tastatur erfolgt).

– `seconds`: Nach `seconds` Sekunden erfolgt der Autologout. Mit Eingabe von `t 0` deaktivieren Sie Autologout.

Durch Eingabe von `-?` erhalten Sie meistens Hilfen zur Syntax.

Das Kommando `update` finden Sie in Kapitel 9.2, Seite 288.

Weitere SNMP-Kommandos finden Sie in der Software Reference.

12.2 BRICKtools for Unix Kommandos

Die Programme bricktrace und capitrace sind in BRICKtools for UNIX auf der BinTec-Companion CD enthalten. Sie werden durch Eingabe der folgenden Kommandos auf einem Unix-Rechner gestartet.

bricktrace

```
bricktrace [-h23aeFpiNtxs] [-T <tei>] [-c <cref>]
[-r <cnt>] [-H <host>] [-P <port>] <channel> <unit> <slot>
```

Wird benutzt, um ISDN-Meldungen (D- und B-Kanäle) zu verfolgen und auszuwerten.

- `-h`: hexadezimale Ausgabe.
- `-2`: Schicht-2-Ausgabe.
- `-3`: Schicht-3-Ausgabe.
- `-a`: Asynchronous HDLC (nur B-Kanal).
- `-e`: ETS300075 (EuroFileTransfer)-Ausgabe.
- `-F`: Fax (nur B-Kanal).
- `-p`: PPP (nur B-Kanal).
- `-i`: IP-Ausgabe (nur B-Kanal).
- `-N`: Novell IPX-Ausgabe (nur B-Kanal).
- `-t`: Ausgabe in ASCII-Text (nur B-Kanal).
- `-x`: Raw dump mode.
- `-s`: **BinGO!** auf verfügbare Trace-Kanäle überprüfen.
- `-T` <tei>: TEI-Filter setzen (nur D-Kanal).
- `-c` <cref>: Callref-Filter setzen (nur D-Kanal).
- `-r` <cnt>: Nur cnt bytes empfangen.
- `-H` <host>: IP-Adresse oder Name des IP-Hosts.
- `-p <port>`: Spezifiziert Trace-TCP-Port (Standard: 7000).
- `channel`: `0` = D-Kanal oder X.21-Schnittstelle, `1` ... `31` Bx-Kanal.
- `unit`: 0 ... 1. Selektieren des physikalischen Interface für Module mit zwei Interfaces (z. B. CM-2BRI).
- `slot`: 1 ... 2. Angabe des Slot, in dem das Modul installiert ist.

capitrace

```
capitrace [-h] [-s] [-l]
```

Wird benutzt, um CAPI-Meldungen zu verfolgen und auszuwerten. Alle von **BinGO!** gesendeten oder empfangenen CAPI-Meldungen werden angezeigt. Als Umgebungs-Variable CAPI_HOST muß die IP-Adresse von **BinGO!** eingegeben werden.

- -h: Hexadezimale Ausgabe (ist standardmäßig eingestellt, wenn keine Optionen spezifiziert werden).
- -s: Kurze Ausgabe. Am Ende der Informationszeile wird lediglich die Applikations-ID, ein connection identifier der Form "(application / identifier)" und der Name der CAPI-Meldung angezeigt.
- -l: Lange Ausgabe (Standard). Eine detaillierte Interpretation jedes Parameters der CAPI-Meldung wird angegeben.

Am Anfang jeder angezeigten CAPI-Meldung stehen die folgenden Informationen:

- Zeitstempel ("Sekunden.Millisekunden" lokaler Zeit)
- Gesendet/Empfangen Flag (X = gesendet, R = empfangen)
- Name der CAPI-Meldung (ASCII-Zeichen)
- Kommando der CAPI-Meldung (0xABXY, AB = <subcommand> XY = <command>)
- Nummer der Tracer-Meldung (#<decimal>)
- Länge der CAPI-Meldung (len = <decimal>)
- Applikations-ID (appl = <decimal>)
- Nummer der CAPI-Meldung (messno = 0x<hexadecimal>)
- Nur bei Kurzer Ausgabe: Connection-Identifier (ident = 0x<hexadecimal>

13 Allgemeine Sicherheitshinweise in 15 verschiedenen Sprachen

General Safety Precautions in English

The following section includes safety precautions you are strongly advised to heed when working with your router.

Transport and storage

- Only transport and store **BinGO!** in its original packaging or use other appropriate packaging to prevent against knocking and shaking.

Placement and operation

- Before setting up this product for operation, please bear in mind the instructions for the most appropriate ambient conditions (cf. technical data). Place on a firm and level surface.
- Condensation may occur externally or internally if this equipment is moved from a colder room to a warmer room. When moving the product under such conditions, allow ample time for the equipment to reach room temperature and to dry completely before operating.
- Make sure the power rating on the label of the mains unit complies with the local power source. **BinGO!** may only be operated with the original BinTec Communications mains unit (5 V DC). BinTec Communications AG accepts no liability for damages caused by the use of other mains units.
- Make sure to follow the correct cabling sequence, as described in the manual. Firstly, connect the LAN, ISDN and serial cables, then connect to the mains, and finally, turn on your **BinGO!**.
- Make doubly sure the cabling is correct – especially the ISDN and LAN cables – before you turn on **BinGO!**. **BinGO!**´s ISDN connection must not be connected with the Ethernet connection of your PC or hub, and neither should **BinGO!**´s LAN connection be connected with the ISDN connection.
- Use only the supplied cables. If you use other cables, BinTec Communications AG can not accept liability for any resulting damage.
- Arrange the cables so as they are not in the way, can not be tripped over and can not be damaged.
- Avoid connecting or disconnecting data lines during lightning storms.

Operate according to the regulations

- **BinGO!** is intended for use in offices. As an ISDN multiprotocol router, **BinGO!** establishes ISDN connections depending on the system configuration. To avoid extra charges, you should carefully monitor the product.
- **BinGO!** corresponds to the relevant safety standards for the use of information technology equipment in offices.
- Operation of the system according to IEC 950/EN 60950 is only guaranteed when the roof of the housing is fitted (cooling, fire-protection, noise suppression)
- Ambient temperature should not exceed 50˚C.
- Make sure no foreign objects (e.g. paper clips) or liquids get into the device (electric shock, short circuit).
- In an emergency (e. g. damaged housing or operating elements, liquid spills or the entry of foreign bodies), immediately remove the AC/DC adaptor and notify customer service.

Cleaning and repair

- The device should only be opened by trained personnel. Only service centers authorized by BinTec should carry out any repairs to the device. Your dealer will tell you where the service centers are situated. As a result of unauthorized opening and improper repairs, serious danger can result for the user (e. g. electric shock). In the event of such non-permissible opening of the device, the terms of the guarantee are suspended and BinTec Communications AG accepts no liability.
- Never use water to clean this device. Water spillage can result in serious danger for the user (electric shock) and cause considerable damage to the device.
- Never use scouring or abrasive alkaline cleaning agents on this device.

Almindelige sikkerhedsforskrifter på dansk

Efterfølgende afsnit indeholder sikkerhedsforskrifter, som skal overholdes, når Deres router benyttes.

Transport og opbevaring

- Transportér og opbevar kun **BinGO!** i originalemballage eller i anden egnet emballage, der beskytter mod stød og slag.

Opstilling og ibrugtagning

- Læs og overhold forskrifterne for de omkringliggende betingelser, før **BinGO!** opstilles og tages i brug (se Tekniske data). Benyt et fast og jævnt underlag.
- Hvis apparatet er koldt, når det bringes ind i brugsrummet, kan der opstå dug i og uden på apparatet. Sørg for at Deres router har rumtemperatur og er absolut tør, før den tages i brug.
- Kontrollér om spændingen på typeskiltet stemmer overens med spændingen på brugsstedet. **BinGO!** må kun arbejde med den originale stiknetdel fra BinTec Communications (5 V DC). BinTec Communications AG fraskriver sig ansvaret for skader, som måtte opstå som følge af brug af en anden stiknetdel.
- Sørg for at kablerne forbindes i den rigtige rækkefølge (se beskrivelsen i manualen). Forbind først LAN-, ISDN- og serielle tilslutninger, tilslut derefter strømforsyningen og tænd til sidst for **BinGO!**.
- Kontrollér om kablerne - især ISDN- og LAN-kablerne - er forbundet rigtigt, før **BinGO!** tages i brug. ISDN-tilslutningen på **BinGO!** må ikke forbindes med Ethernet-tilslutningen på Deres computer eller hub og LAN-tilslutningen på **BinGO!** må ikke forbindes med Deres ISDN-tilslutning.
- Apparatet må kun forbindes med vedlagte kabler. Hvis De benytter andre kabler, fraskriver BinTec Communications AG sig ansvaret for evt. skader.
- Ledningerne skal trækkes på en sådan måde, at de ikke beskadiges og at de ikke er til fare for omgivelserne (fare for at snuble).
- Tilslut ikke datatransmissionsledninger og træk dem ikke ud af apparatet, når det er tordenvejr.

Beregnet anvendelse-område, brug

- **BinGO!** er beregnet til at blive brugt på kontorer. **BinGO!** opbygger som ISDN-multi-protokol-router ISDN-forbindelser afhængigt af systemkonfigurationen. De bør overvåge produktet for at undgå uønskede gebyrer.
- **BinGO!** overholder gældende sikkerhedsbestemmelser mht. indretning af informationsteknik til kontorer.
- Den beregnede brug af systemet (iht. IEC 950/EN 60950) er kun sikret, når låget er monteret på huset (køling, brandbeskyttelse, radiostøjdæmpning)
- Omgivelsestemperaturen må ikke overstige 50˚C. Undgå direkte solstråler.
- Vær opmærksom på, at genstande (f.eks. klips) eller væske ikke trænger ind i apparatet (elektrisk stød, kortslutning). Sørg for tilstrækkelig køling.
- Afbryd straks strømforsyningen og kontakt serviceafdelingen i nødstilfælde (f.eks. beskadiget hus eller betjeningselement, indtrængning af væske eller fremmede genstande).

Rengøring og reparation

- Apparatet må kun åbnes af skolet fagligt personale. Reparationer på apparatet skal derfor altid udføres på et autoriseret BinTec serviceværksted. Deres forhandler kan oplyse om det nærmeste serviceværksted. Ubeføjet åbning og ukorrekte reparationer kan udsætte brugeren for stor fare. BinTec Communications AG fraskriver sig ethvert ansvar og garantien bortfalder, hvis apparatet åbnes uden tilladelse.
- Apparatet må under ingen omstændigheder rengøres med væske. Indtrængende vand kan udsætte brugeren for alvorlige farer (f.eks. elektrisk stød) og alvorlige skader på apparatet.
- Benyt aldrig skuremidler, alkaliske rengøringsmidler, skrappe eller skurende hjælpemidler.

Yleiset turvallisuusmääräykset

Seuraavista kappaleista löydät turvallisuusmääräykset, joita on ehdottomasti noudatettava reittivalitsinta käytettäessä.

Kuljetus ja varastointi

- Kuljeta ja varastoi **BinGO!** vain alkuperäispakkauksessaan tai muussa sopivassa pakkauksessa, joka suojaa töytäisyiltä ja iskuilta.

Asennus ja käyttöönotto

- Tarkista ennen **BinGO!** -laitteen asennusta ja käyttöä, että ympäristöolosuhteista annettuja ohjeita (kts. lukua Tekniset tiedot) on noudatettu. Aseta laite tukevalle, tasaiselle alustalle.
- Kun laite tuodaan kylmästä tilasta käyttötiloihin, voi sekä laitteen ulkopinnalla että sen sisäpuolella esiintyä tiivistynyttä vettä. Odota siksi, kunnes reittivalitsimen lämpötila on noussut huonelämpöön ja se on ehdottoman kuiva, ennen kuin otat sen käyttöön.
- Tarkasta, että verkkolaitteen tyyppikilvessä annettu verkkojännite on sama kuin paikallinen verkkojännite. **BinGO!** -laitetta saa käyttää vain alkuperäisen BinTec Communications-pistokeverkkolaitteen (5 V DC) kanssa. BinTec Communications AG ei vastaa vahingoista, jotka ovat aiheutuneet muun pistokeverkkolaitteen käytöstä.
- Käsikirjassa kuvattua kaapelien liitäntäjärjestystä on ehdottomasti noudatettava. Yhdistä ensin LAN-, ISDN- ja sarjaliitännät, liitä laite sitten virtaverkkoon ja kytke lopuksi **BinGO!** päälle.
- Tarkasta, että olet liittänyt kaapelit oikein, erityisesti ISDN- ja LAN-kaapelit, ennen kuin käynnistät **BinGO!** -laitteen. **BinGO!** -laitteen ISDN-liitäntää ei saa liittää laskimen tai jakajan Ethernet-liitäntään eikä **BinGO!** -laitteen LAN -liitäntää saa yhdistää ISDN-liitäntääsi.
- Käytä laitteiden yhdistämiseen vain mukanatoimitettuja kaapeleita. Jos käytät muita kaapeleita, ei BinTec Communications AG vastaa tästä aiheutuvista vahingoista.
- Vedä kaapelit sellaisiin paikkoihin, että ne eivät aiheuta vaaratilanteita (kompastumisia) eivätkä vahingoitu.
- Ukkosen aikana ei tietoliikennekaapeleita tule liittää eikä myöskään irroittaa.

Määräystenmukainen käyttö, käyttö

- **BinGO!** on suunniteltu käytettäväksi toimistotiloissa. **BinGO!** toimii ISDN-monikäytäntö-reittiohjaimena ja luo järjestelmän konfiguraation mukaisesti ISDN-yhteyksiä. Epätoivottujen maksujen välttämiseksi on tuotteen toimintaa välttämättä valvottava.
- **BinGO!** vastaa toimistotiloissa käytettäville tietotekniikan laitteistoille asetettuja asiaankuuluvia turvallisuusmääräyksiä.
- Järjestelmän määräystenmukainen käyttö standardin IEC 950/EN 60950 mukaan on mahdollista vain kun kotelon kansi on asennettu paikalleen (jäähdytys, palosuojelu, häirintäsuojaus)
- Ympäristön lämpötila ei saisi nousta yli 50˚C. Älä aseta laitetta alttiiksi suoralle auringonpaisteelle.
- Varo, ettei mitään vieraita esineitä (esim. paperiliittimiä) tai nesteitä pääse laitteen sisäpuolelle (sähköisku, lyhytsulku). Huolehdi siitä, että laitteen jäähdytys on riittävä.
- Keskeytä hätätilanteessa (esim. särkynyt kotelo tai käyttölaite, nesteen tai vieraiden esineiden joutuminen laitteen sisään) virransyöttö välittömästi ja ota yhteyttä huoltopalveluun.

Puhdistus ja korjaus

- Vain koulutettu ammattihenkilöstö saa avata laitteen. Anna sen vuoksi kaikki korjaustyöt vain BinTec-valtuutetun huoltokorjaamon tehtäväksi. Kauppiaasi voi kertoa, missä on lähin valtuutettu huoltokorjaamo. Luvaton aukaiseminen ja asiantuntemattomat korjaukset saatttavat aiheuttaa käyttäjälle vakavia vaaratilanteita (esim. sähköisku). Laitteiden luvaton aukaiseminen aiheuttaa BinTec Communications AG -takuun raukeamisen sekä kaikkinaisen vastuun epäämisen.
- Älä missään tapauksessa puhdista laitetta runsaalla vedellä. Sen sisään tunkeutunut vesi saattaisi aiheuttaa vakavia vaaroja (sim. sähköisku) käyttäjälle ja vaurioittaa laitetta pahasti.
- Älä koskaan käytä puhdistamiseen hankausaineita, alkalisia puhdistusaineita taikka syövyttäviä tai hankaavia tehoaineita.

Consignes de sécurité générales en français

Vous trouverez, dans les paragraphes suivants, les consignes de sécurité que vous devez absolument respecter lors de l'utilisation de votre router.

Transport et entreposage

- Transportez et entreposez **BinGO!** uniquement dans son emballage d'origine ou dans un autre emballage approprié lui garantissant une bonne protection contre les chocs et les coups.

Installation et mise en service

- Avant de procéder à l'installation et à la mise en service de **BinGO!** , veillez aux indications concernant les conditions d'environnement (cf. Caractéristiques techniques). Utilisez un support stable et plan.
- Lorsque vous transportez l'appareil d'un environnement froid jusqu'à la salle dans laquelle il fonctionnera, une rosée peut se former aussi bien sur la paroi extérieure de l'appareil qu'à l'intérieur de ce dernier. Attendez jusqu'à ce que votre Router ait atteint la température ambiante et jusqu'à ce qu'il soit absolument sec avant de le mettre en service.
- Vérifiez si la tension nominale indiquée sur la plaque signalétique du bloc d'alimentation correspond bien à la tension de l'endroit en question. **BinGO!** doit uniquement fonctionner avec la fiche du bloc d'alimentation BinTec Communications originale (5 V DC). BinTec Communications AG décline toute responsabilité pour les dommages dus à l'utilisation d'une autre fiche de bloc d'alimentation.
- Lors du câblage, respectez l'ordre tel qu'il est indiqué dans le manuel. Câblez tout d'abord les raccordements LAN, ISDN et sériels, établissez ensuite la connexion avec le courant et mettez finalement **BinGO!** en service.
- Vérifiez si vous avez bien effectué le câblage, en particulier celui de ISDN et LAN, avant de mettre **BinGO!** en service. Le raccordement ISDN de **BinGO!** ne doit pas être relié au raccordement Ethernet de votre ordinateur ou de votre borne, le raccordement LAN de **BinGO!** ne doit pas être relié à votre raccordement ISDN.
- Utilisez uniquement les câbles joints à la livraison pour effectuer le câblage. Dans le cas où vous utilisez d'autres câbles que ces derniers, BinTec Communications AG décline toute responsabilité pour tout dommage qui pourrait en découler.

- Posez les câbles de telle sorte qu'ils ne puissent pas être à l'origine de risques (risques de trébuchement) ni ne puissent être endommagés.
- Ne connectez pas ni ne déconnectez les câbles de transmission de données pendant un orage.

Utilisation conforme à l'affectation prévue, fonctionnement

- **BinGO!** est prévu pour être employé dans les bureaux. **BinGO!** établit des connexions ISDN qui dépendent de la configuration du système en tant que routeur ISDN Multi à procès-verbal. Pour éviter de payer des taxes inconsidérément, vous devriez absolument surveiller ce produit.
- **BinGO!** est conforme aux prescriptions de sécurité correspondantes relatives aux équipements de la technique de l'information pour l'emploi en bureau.
- L'emploi de ce système conforme à l'affectation prévue, conformément à la norme IEC 950/EN 60950 n'est garantit que si le couvercle du boîtier est monté (refroidissement, protection anti-incendie, étincelles)
- La température ambiante ne doit pas dépasser 50˚C. Evitez le rayonnement direct du soleil sur l'appareil.
- Veillez à ce qu'aucun objet (par ex. des agrafes) ni aucun liquide ne s'introduise à l'intérieur de l'appareil (électrocution, court-circuit). veillez à ce que l'appareil soit suffisamment refroidi.
- Dans les cas d'urgence extrême (par ex. si le boîtier ou des éléments de commande sont endommagés, si du liquide ou des corps étrangers se sont introduits dans l'appareil), déconnectez immédiatement l'alimentation en courant et prévenez le service.

Nettoyage et Réparation

- L'appareil doit être ouvert uniquement par un personnel spécialisé dûment instruit. Ne faites donc réaliser les réparations de l'appareil que par un poste de service autorisé BinTec. Votre concessionnaire vous fera part de l'adresse à laquelle vous pourrez contacter ce service. Des risques très importants pour l'opérateur (par ex. électrocution) peuvent naître à cause d'une ouverture non autorisée et de réparations non conformes aux règles de l'art. Le fait d'ouvrir l'appareil sans autorisation rend caduque toute clause de garantie et de responsabilité de la part de la BinTec Communications AG.

- L’appareil ne doit être en aucun cas nettoyé à l’eau. Une introduction de l’eau dans l’appareil pourrait entraîner des risques énormes pour l’opérateur (par ex. électrocution) et des dommages importants de l’appareil pourraient en être la conséquence.
- Ne jamais utiliser de produits récurants, de produits de nettoyage alcalins, ni de produits auxiliaires tranchants ou grattants.

2 Γενικές οδηγίες ασφαλείας στα Ελληνικά

Στις ακόλουθες παραγράφους θα βρείτε τις οδηγίες ασφαλείας, τις οποίες θα πρέπει να λάβετε οπωσδήποτε υπ' όψιν σας κατά τη χρήση του Router.

Μεταφορά και αποθήκευση

- Να μεταφέρετε και να αποθηκεύετε το **BinGO!** μόνο στη γνήσια συσκευασία ή σε μία άλλη κατάλληλη συσκευασία, η οποία να εξασφαλίζει προστασία κατά των κρούσεων και χτυπημάτων.

Στήσιμο και έναρξη της λειτουργίας

- Πριν το στήσιμο και την έναρξη της λειτουργίας του **BinGO!** να λάβετε υπ' όψιν σας τις οδηγίες σχετικά με τις περιβαλλοντολογικές συνθήκες (βλέπε Τεχνικά στοιχεία). Χρησιμοποιήστε ένα σταθερό και επίπεδο υπόβαθρο.
- Όταν η συσκευή μεταφέρεται από ψυχρό περιβάλλον στο χώρο λειτουργίας, μπορεί να κατακαθίσει υγρασία στο εξωτερικό της συσκευής καθώς και στο εσωτερικό της ίδιας. Να κάνετε υπομονή, μέχρι που η θερμοκρασία του Router να έχει προσαρμοστεί και η συσκευή να είναι τελείως στεγνή, προτού να τη θέσετε εκ νέου σε λειτουργία.
- Επανελέγξτε εάν η ονομαστική τάση που αναφέρεται στην πλακέτα τύπου του φις αντιστοιχεί στην κατά τόπους τάση του δικτύου. Το **BinGO!** επιτρέπεται να λειτουργεί μόνο με το γνήσιο φις BinTec Communications (5 V DC). Η BinTec Communications AG δεν ευθύνεται για ζημιές που ενδέχεται να προκληθούν από τη χρήση ενός άλλου φις.
- Προσέξτε κατή την καλωδίωση, ώστε να τηρηθεί η σωστή σειρά που περιγράφεται στο εγχειρίδιο. Καλωδιώστε κατ' αρχήν το LAN, το ISDN και τη σειριακή διεπαφή. Στη συνέχεια να γίνεται η σύνδεση με το ηλεκτρικό ρεύμα και στο τέλος θέστε το **BinGO!** σε λειτουργία.
- Επανελέγξτε εάν καλωδιώσατε κατά τον προβλεπόμενο τρόπο ιδίως το ISDN και το LAN, προτού να θέσετε το **BinGO!** σε λειτουργία. Η σύνδεση ISDN του **BinGO!** δεν επιτρέπεται να συνδεθεί με τη σύνδεση Ethernet του υπολογιστή ή της υποδοχής σας, και η

σύνδεση LAN του **BinGO!** δεν επιτρέπεται να συνδεθεί με τη σύνδεση ISDN.

- Χρησιμοποιήστε για την καλωδίωση μόνον τα συνημμένα καλώδια. Σε περίπτωση που χρησιμοποιήσετε άλλα καλώδια, η BinTec Communications AG δεν αναλαμβάνει καμία ευθύνη για ενδεχόμενες προκληθείσες ζημιές.
- Διαστρώστε το δίκτυο κατά τέτοιον τρόπο, ώστε να μην προκύψουν σημεία κινδύνου (κίνδυνος παραπατήματος) και ώστε να μη μπορεί να υποστεί ζημιά.
- Μη συνδέετε και μην αποχωρίζετε κατά τη διάρκεια μιας καταιγίδας αγωγούς μεταφοράς δεδομένων.

Προβλεπόμενη χρήση, λειτουργία

- Το **BinGO!** προβλέπεται για τη χρήση σε περιβάλλον γραφείου. Ως Router ποικίλων προτοκόλλων ISDN το **BinGO!** εγκαθιστά συνδέσεις σε συνάρτηση με τη σύνθεση του συστήματος ISDN. Για να αποφύγετε την κατάπτωση ακούσιων τελών, θα έπρεπε το προϊόν οπωσδήποτε να επιβλέπεται.
- Το **BinGO!** ανταποκρίνεται στις σχετικές διατάξεις ασφαλείας για εγκαταστάσεις της τεχνολογίας πληροφοριών κατά τη χρήση σε περιβάλλον γραφείου.
- Η προβλεπόμενη λειτουργία του συστήματος σύμφωνα με την IEC 950/EN 60950 διασφαλίζεται μόνον, όταν το καπάκι του κελύφους είναι μονταρισμένο (ψύξη, αντιπυρική προστασία, παρεμβολή σπινθήρων).
- Η περιβαλλοντολογική θερμοκρασία δε θα έπρεπε να υπερβαίνει τους 50°C. Αποφύγετε την έκθεση σε άμεση ηλιακή ακτινοβολία.
- Να προσέχετε, ώστε να μην εισέλθουν αντικείμενα (π.χ. συνδετήρες) ή υγρά στο εσωτερικό της συσκευής (κίνδυνος ηλεκτροπληξίας, βραχυκυκλώματος). Θα πρέπει να εξασφαλίζεται η επαρκής ψύξη.
- Να διακόπτετε σε έκτακτες περιπτώσεις (π.χ. όταν έχει προκληθεί βλάβη στο κέλυφος ή στη μονάδα χειρισμού ή όταν έχουν εισέλθει υγρά ή αντικείμενα) αμέσως την παροχή ρεύματος και να έρχεστε σε επαφή με το κατάλληλο συνεργείο.

Καθαρισμός και επισκευή

- Η συσκευή επιτρέπεται να ανοίγεται μόνον από ειδικά εκπαιδευμένο τεχνικό προσωπικό. Γι' αυτόν το λόγο να επιτρέπεται τη διεξαγωγή εργασιών επισκευής μόνο σε συνεργεία που έχου εξουσιοδοτηθεί από την BinTec. Σχετικά με την έδρα των σχετικών συνεργείων μπορείτε να ζητήσετε πληροφορίες από τον εμπορικό σας αντιπρόσωπο. Το άνοιγμα της συσκευής από αναρμόδια άτομα καθώς και ακατάλληλες εργασίες επισκευής μπουρούν να θέσουν το χρήστη σε σοβαρούς κινδύνους (π.χ. ηλεκτροπληξία). Το ανεπίτρεπτο άνοιγμα της συσκευής έχει σαν αποτέλεσμα την αποποίηση κάθε εγγύησης και ευθύνης από μέρους της BinTec Communications AG.
- Η συσκευή δεν επιτρέπεται σε καμία περίπτωση να καθαριστεί. Από την ενδεχόμενη είσοδο νερού μπορεί να προκύψουν σημαντικοί κίνδυνοι για το χρήστη (π.χ. ηλεκτροπληξία) και σοβαρές ζημιές στη συσκευή.
- Να μη χρησιμοποιείτε ποτέ μέσα που προβλέπονται για το τρίψιμο, αλκαλικά απορρυπαντικά μέσα και αιχμηρά ή αδρά βοηθητικά μέσα καθαρισμού.

Istruzioni generali di sicurezza

Nei seguenti paragrafi si trovano elencate le istruzioni generali di sicurezza da osservare rigorosamente nell'uso del Suo Router.

Trasporto e magazzinaggio

- Trasporti ed immagazzini **BinGO!** soltanto nell'imballaggio originale o in altro imballaggio adeguato a garantire protezione da urti e scotimenti.

Installazione e azionamento

- Prima di installare ed azionare **BinGO!** faccia attenzione alle istruzioni sulle condizioni ambientali (cfr. Dati tecnici). Utilizzi un ripiano stabile e piano.
- Se l'apparecchio viene introdotto nel locale di funzionamento da un ambiente freddo può verificarsi una condensa sia all'interno che all'esterno dell'apparecchio. Aspetti che il Suo Router si sia adeguato alla temperatura e che sia perfettamente asciutto prima di azionarlo.
- Controlli che la tensione indicata sulla targhetta della sezione di rete corrisponda alla tensione di rete locale. **BinGO!** può essere azionato soltanto con la spina di sezione di rete originale BinTec Communications (5 V DC) La BinTec Communications AG non risponde dei danni causati dall'utilizzo di una spina di sezione di rete diversa.
- Nel cablare osservi l'ordine di successione descritto nel manuale. Cabli prima i collegamenti LAN-, ISDN- e quelli seriali, colleghi poi al distributore di corrente ed alla fine azioni **BinGO!** .
- Controlli di aver eseguito il cablaggio correttamente – in particolare quello ISDN- e LAN- prima di azionare **BinGO!** . Il collegamento ISDN di **BinGO!** non deve essere collegato al collegamento Ethernet del Suo computer o dell'Hub, il collegamento LAN-di **BinGO!** non deve essere collegato al Suo collegamento ISDN.
- Utilizzi per il cablaggio soltanto i cavi allegati.. Nel caso in cui si utilizzino cavi diversi, la BinTec Communications AG non risponde per i danni che ne derivino.
- Disponga i collegamenti in modo che non costituiscano fonte di pericolo (pericolo d'inciampo) e che non possano essere danneggiati.
- Non colleghi nè scolleghi i collegamenti di trasmissione dati durante un temporale.

Utilizzazione conforme a destinazione, funzionamento

- **BinGO!** è destinato ad essere impiegato in ambiente d'ufficio. Quale ISDN-Multi-Protokoll-Router istituisce **BinGO!** collegamenti ISDN in dipendenza della configurazione di sistema. Onde evitare conteggi indesiderati dovrebbe assolutamente sorvegliare il prodotto.
- **BinGO!** è conforme alle relative disposizioni di sicurezza per impianti della tecnica informatica impiegati in ambiente d'ufficio.
- Il funzionamento conforme a destinazione secondo IEC 950/EN 60950 del sistema è garantito soltanto a coperchio montato sulla cassetta (raffreddamento, protezione antincendio, schermatura contro radio disturbi)
- La temperatura ambientale non dovrebbe superare i 50˚C. Eviti l'esposizione diretta alla luce solare.
- Faccia attenzione che nessun oggetto (p.es. fermagli) o liquido si insinui all'interno dell'apparecchio (scossa elettrica, corto circuito). Faccia attenzione ad un sufficiente raffreddamento.
- In casi d'emergenza (p.es. danneggiamento della scatola o dell'elemento servente/manovrante, infiltrazione di liquido o di corpi estranei) stacchi immediatamente la corrente ed informi il servizio assistenza.

Pulizia e riparazione

- L'apparecchio può essere aperto soltanto da personale competente ed addestrato. Si consiglia pertanto di far riparare l'apparecchio soltanto presso un centro assistenza autorizzato BinTec. Gli indirizzi dei servizi assistenza sono a disposizione presso il Suo rivenditore. Apertura non autorizzata e riparazioni inappropriate possono essere fonte di gravi pericoli per l'utente (p.es. scossa elettrica). Un'apertura non autorizzata degli apparecchi comporta l'esclusione della garanzia e della responsabilità della BinTec Communications AG .
- L'apparecchio non deve assolutamente essere pulito con acqua. L'infiltrazione di acqua può causare gravi pericoli per l'utente (p.es. scossa elettrica) nonché gravi danni all'apparecchio.
- Non utilizzi in nessun caso abrasivi, detersivi a base alcalina, detersivi corrosivi o abrasivi.

Algemene veiligheidsinstructies in het Nederlands

In de volgende paragrafen vindt u veiligheidsinstructies, die u bij de omgang met uw router absoluut moet in acht nemen.

Transport en bewaring

- Transporteert en bewaart u **BinGO!** alleen in de originele verpakking of in een andere geschikte verpakking, die bescherming biedt tegen schokken en stoten.

Opstellen en in bedrijf nemen

- Let voor het opstellen en het bedrijf van **BinGO!** op de instructies voor de omgevingsvoorwaarden (vergelijk technische gegevens). Gebruikt u een harde en vlakke ondergrond.
- Wanneer het apparaat uit een koude omgeving in de werkruimte wordt gebracht, kan er zowel uitwendig op als inwendig in het apparaat condensatie optreden. Wacht u tot uw router is aangepast aan de temperatuur en tot hij volledig droog is, voordat u hem in bedrijf neemt.
- Controleert u, of de op het typeplaatje aangegeven nominale spanning overeenstemt met de plaatselijke netspanning. **BinGO!** mag alleen met de originele BinTec Communications elektrische stekkervoeding (5 V DC) worden gebruikt. BinTec Communications AG is niet aansprakelijk voor beschadigingen, die ontstaan door gebruik van een andere elektrische voeding.
- Let bij de aansluiting van de kabels op de volgorde, zoals in het handboek wordt beschreven. Eerst sluit u de LAN-, ISDN- en de seriële aansluitingen aan, sluit daarna de stroomverzorging aan, en tenslotte schakelt u **BinGO!** in.
- Controleert u, of u de aansluiting - in het bijzonder de ISDN- en LAN-aansluiting correct heeft uitgevoerd, alvorens u **BinGO!** in bedrijf neemt. De ISDN-aansluiting van **BinGO!** mag niet met de ethernet-aansluiting van uw computer of hub go-ahead worden verbonden, de LAN-aansluiting van **BinGO!** niet met uw ISDN-aansluiting.
- Gebruikt u voor de aansluiting slechts de bijgevoegde kabels. Indien u andere kabels gebruikt, is BinTec Communications AG niet aansprakelijk voor optredende schade.

- Leg de kabels zodanig, dat zij geen gevaarsbron (struikelgevaar) vormen en niet worden beschadigd.
- Koppel de datatransfertkabels nooit aan of af tijdens een onweer.

Doelmatig gebruik, bedrijf

- **BinGO!** is bestemd voor toepassing in een kantooromgeving. Als ISDN-Multi-Protocol-Router maakt **BinGO!** afhankelijk van de systeemconfiguratie ISDN-verbindingen. Om ongewenste kosten te vermijden, dient u het product absoluut te bewaken.
- **BinGO!** voldoet aan de gebruikelijke veiligheidsbepalingen voor inrichtingen van informatietechniek voor toepassing in een kantooromgeving.
- Het doelmatig bedrijf, overeenkomstig IEC 950/EN 60950 van het systeem, is alleen bij gemonteerd huisdeksel gewaarborgd (koeling, brandveiligheid, vonkontstoring)
- De omgevingstemperatuur mag niet hoger zijn dan 50˚C. Vermijdt u direct zonlicht.
- Let erop, dat er geen voorwerpen (bijv. paperclips) of vloeistoffen in het inwendige van het apparaat geraken (elektrische schok, kortsluiting). Let u op voldoende koeling.
- Onderbreekt u in noodgevallen (bijv. beschadigd huis, of bedienelement, binnendringen van vloeistof of vreemde voorwerpen) onmiddellijk de stroomverzorging en neemt u contact op met de service-dienst.

Reiniging en reparatie

- Het apparaat mag alleen door geschoold vakpersoneel worden geopend. Laat u daarom reparaties aan het apparaat alleen uitvoeren door een door BinTec-geautoriseerde service-dienst. Waar zich deze service-dienst bevindt, ervaart u bij uw handelaar. Door het onbevoegde openen en ondeskundige reparaties kunnen aanzienlijke gevaren ontstaan voor de gebruiker (bijv. elektrische schok). Onbevoegd openen van de apparaten heeft verval van de garantie en uitsluiting van de aansprakelijkheid van de BinTec Communications AG tot gevolg.
- Het apparaat mag in geen geval nat worden gereinigd. Door binnendringend water kunnen er aanzienlijke gevaren ontstaan voor de gebruiker (bijv. elektrische schok) en kan er aanzienlijke schade ontstaan aan het apparaat.

- Gebruikt u nooit schuurmiddelen, alkalische reinigingsmiddelen, scherpe of schurende hulpmiddelen.

Generelle sikkerhetshenvisninger på norsk

I de følgende avsnittene finner du sikkerhetshenvisninger som du absolutt må ta hensyn til ved omgangen med din Router.

Transport og lagring

- Du må kun transportere og lagre **BinGO!** i originalemballasjen eller i en annen egnet emballasje som beskytter mot støt og slag.

Oppstilling og ibruktaking

- Før oppstilling og drift av **BinGO!** må du ta hensyn til henvisningene når det gjelder omgivelsesbetingelsene (sml. tekniske data). Bruk et fast og jevnt underlag.
- WDersom apparatet blir tatt fra en kald omgivelse og inn i rommet der det skal brukes, kan det oppstå kondens både på utsiden og på innsiden av apparatet. Vent til Router har tilpasset seg temperaturen og er helt tørr før du tar den i bruk.
- ÜKontroller om den spenningen som er oppgitt på typeskiltet på nettdelen stemmer overens med spenningen på stedet. **BinGO!** må kun brukes sammen det originale BinTec kommunikasjons-støpselet (5 V DC). BinTec Communications AG er ikke ansvarlig for skader som måtte oppstå på grunn av at det er blitt brukt en annen støpsel-nettdel.
- Ved sammenkopling av kablene, må det tas hensyn til rekkefølgen som er beskrevet i håndboken. Sammenkople først kablene LAN-, ISDN- og serielle tilkoplinger, tilkople så strømforsyningen, og slå deretter til slutt på **BinGO!** .
- Kontroller om du har foretatt sammenkoplingen av kablene skikkelig– i særdeleshet ISDN- og LAN-sammenkoplingen, før du tar **BinGO!** i drift. ISDN-tilkoplingen fra **BinGO!** må ikke forbindes med Ethernet-tilkoplingene på datamaskinen eller med Hubs, og LAN-tilkoplingen må ikke forbindes med **BinGO!** ISDN-tilkoplingen.
- Bruk kun de vedlagte kablene for sammenkabling. Dersom du bruker andre kabler, overtar BinTec Communications AG intet ansvar for skader som måtte oppstå av den grunn.
- Legg opp ledningene slik at de ikke kan bli skadet og at de ikke danner farekilder (fare for å snuble) .

- Under tordenvær må du hverken tilkople eller trekke av noen av dataoverføringsledningene.

Forskriftsmessig bruk, drift

- **BinGO!** er beregnet for innsats på kontoromgivelser. Som ISDN-Multi-Protokoll-Router bygger **BinGO!** opp ISDN-forbindelser i avhengighet av systemkonfigurasjonen. For å unngå uønskede gebyrer, bør produktet absolutt overvåkes.
- **BinGO!** tilsvarer de gyldige sikkerhetsbestemmelsene for innretninger innenfor informasjonsteknikken for innsats i en kontoromgivelse.
- Den forskriftsmessige bruken i henhold til IEC 950/EN 60950 for systemet er kun garantert ved montert maskinkasse (Kjøling, brannbeskyttelse, fjerning av radiostøy)
- Omgivelsestemperaturen bør ikke overstige 50˚C. Unngå direkte sollys.
- Pass på at ingen gjenstander (f. eks. binders) eller væsker kan komme inn i apparatet (fare for elektrisk støt, kortslutning). Pass på tilstrekkelig avkjøling.
- I nødstilfeller (z. B. skadet kasse eller betjenings-elementer, når væske eller fremmedlegemer er kommet inn) må du straks avbryte strømforsyningen og tilkalle service.

Rengjøring og reparasjon

- Apparatet må kun åpnes av opplært fagpersonell. La derfor alltid reparasjoner på apparatet gjennomføres av et BinTec-autorisert serviceverksted.. Din forhandler informerer det om hvor du finner serviceverksteder. Dersom uvedkommende åpner eller reparerer apparatet, kan det oppstå stor skade for brukeren (f. eks. strømstøt). Dersom apparatet blir ulovlig åpnet, kan ha til følge at garantien mistes, og at ethvert ansvar blir utelukket fra BinTec Communications AG .
- Apparatet må under ingen omstendigheter rengjøres med vann. Dersom vannet trenger inn, kan det oppstå alvorlige skader for brukeren (f. eks. strømstøt) og også på apparatet.
- Bruk aldri skuremidler, alkaliske rengjøringsmidler, skarpe eller skurende hjelpemidler.

2 Ogólne zasady bezpieczeństwa w języku polskim

Poniżej podano zasady bezpieczeństwa, których należy bezwzględnie przestrzegać przy obchodzeniu się z routerem.

Transport i magazynowanie

- Urządzenie **BinGO!** należy transportować i magazynować wyłącznie w opakowaniu oryginalnym lub innym nadającym się do tego celu opakowaniu, zapewniającym ochronę przed obiciami i uderzeniami.

Ustawianie i uruchamianie

- Przed ustawieniem i uruchomieniem urządzenia **BinGO!** należy zastosować się do wskazówek dotyczących warunków otoczenia (por. Parametry techniczne). Urządzenie należy ustawić na trwałym i równym podłożu.
- Po przeniesieniu urządzenia z zimnego otoczenia do pomieszczenia roboczego zarówno we wnętrzu, jak i na częściach zewnętrznych urządzenia może się tworzyć rosa. Przed uruchomieniem routera należy odczekać na zrównanie się jego temperatury z temperaturą pomieszczenia i jego całkowite wyschnięcie.
- Należy sprawdzić, czy podane na tabliczce typologicznej zasilacza napięcie znamionowe jest zgodne z lokalnym napięciem sieciowym. Urządzenie **BinGO!** można eksploatować wyłącznie w połączeniu z oryginalnym zasilaczem wtykowym produkcji firmy BinTec Communications (5 V DC). Firma BinTec Communications AG nie odpowiada za szkody wywołane stosowaniem zasilacza innego typu.
- Przy przyłączaniu przewodów należy przestrzegać kolejności opisanej w instrukcji obsługi. W pierwszej kolejności należy przyłączyć złącza LAN, ISDN oraz złącza seryjne, następnie włączyć zasilanie prądem elektrycznym, na koniec zaś włączyć router **BinGO!**.
- Przed uruchomieniem urządzenia **BinGO!** należy sprawdzić, czy przyłączenie przewodów - a w szczególności przewodów ISDN i LAN - jest prawidłowe. Złącze ISDN urządzenia **BinGO!** nie może być połączone ze złączem eternetowym komputera lub koncentratora, zaś złącze LANurządzenia **BinGO!** ze złączem ISDN.

- Do przyłączenia produktu należy zastosować wyłącznie dostarczone wraz z nim przewody. W przypadku zastosowania innych przewodów firma BinTec Communications AG nie ponosi odpowiedzialności za powstałe szkody.
- Przewody należy ułożyć tak, aby nie występowało niebezpieczeństwo potykania się o nie oraz ich uszkadzania.
- Podczas burzy nie należy przyłączać ani odłączać przewodów transmisji danych.

Zgodne z przeznaczeniem stosowanie, eksploatacja

- Urządzenie **BinGO!** jest przeznaczone do stosowania w otoczeniach biurowych. Jako router multiprotokołowy ISDN urządzenie **BinGO!** wykonuje połączenia typu ISDN w zależności od konfiguracji systemu. W celu unikania niepożądanych opłat należy koniecznie nadzorować produkt.
- Urządzenie **BinGO!** spełnia obowiązujące zasady bezpieczeństwa dla urządzeń informatycznych przeznaczonych do stosowania w otoczeniu biurowym.
- Zgodne z przeznaczeniem użytkowanie systemu według wymogów norm IEC 950/EN 60950 jest zagwarantowane tylko przy zamontowanej pokrywie obudowy (chłodzenie, zabezpieczenie przeciwpożarowe, eliminacja zakłóceń)
- Temperatura otoczenia nie powinna przekraczać 50°C. Należy unikać bezpośredniego działania promieni słonecznych.
- Należy uważać, aby do wnętrza urządzenia nie wnikały żadnego rodzaju przedmioty (np. spinacze biurowe) bądź ciecze (udar prądowy, zwarcia). Zapewnić wystarczające chłodzenia urządzenia.
- W sytuacjach awaryjnych (np. uszkodzona obudowa lub elementobsługi, wniknięcie cieczy bądź ciał obcych) należy natychmiast przerwać zasilanie urządzenia prądem elektrycznym i zawiadomić serwis.

Oczyszczanie i naprawa

- Urządzenie może być otwierane tylko przez odpowiednio przeszkolony personel. Naprawy urządzenia należy w związku z tym zlecać wyłącznie autoryzowanym przez firmę BinTec punktom serwisowym. Informacji na temat lokalizacji tych punktów można zasięgnąć w punkcie sprzedaży. Otwieranie obudowy urządzenia bez upoważnienia lub jego niefachowe naprawy mogą wywoływać poważne zagrożenia dla użytkownika (np.

porażenie prądem). Niedozwolone otwieranie urządzeń pociąga za sobą utratę gwarancji udzielanej przez firmę BinTec Communications AG oraz jej odpowiedzialności cywilnej za skutki użytkowania produktu.

- Urządzenia pod żadnym pozorem nie wolno czyścić na mokro. Dostanie się wody do wnętrza urządzenia może wywoływać poważne zagrożenia dla użytkownika (np. porażenie prądem) oraz poważne uszkodzenia produktu.
- Nigdy nie stosować środków do szorowania, zasadowych środków czyszczących, ostrych lub szorujących środków pomocniczych.

Considerações genéricas em matéria de segurança em português

Nos parágrafos que se seguem, encontra considerações em matéria de segurança que terá de respeitar estritamente ao lidar com o Router.

Transporte e armazenamento

- Transporte e armazene o **BinGO!** apenas na embalagem original ou noutra adequada para o efeito que o proteja contra embates fortes e pancadas.

Instalação e colocação em funcionamento

- Antes de proceder à instalação e à colocação em funcionamento do **BinGO!** tenha em conta as indicações relativas às condições ambientais (cf. Dados técnicos). Utilize uma base consistente e lisa.
- Ao trazer o aparelho de um ambiente frio para a sala de trabalho, podem formar-se gotículas tanto no exterior, como no interior do aparelho. Espere até que o Router fique à temperatura da sala e absolutamente seco, antes de o pôr a funcionar.
- Verifique se a tensão nominal constante da placa de características da fonte de alimentação é a mesma da do local. O **BinGO!** só pode ser colocado em funcionamento com a ficha da fonte de alimentação BinTec Communications (5 V DC) original. A BinTec Communications AG não se responsabiliza por danos decorrentes da utilização de outra ficha de fonte de alimentação.
- Ao proceder à cablagem, respeite a sequência, tal como descrito no manual. Proceda primeiro à distribuição das ligações LAN, RDIS e em série, conecte depois a alimentação de corrente e, para terminar, ligue o **BinGO!**.
- Verifique se a cablagem, em especial da RDIS e da LAN, ficou bem feita, antes de pôr o **BinGO!** em funcionamento. A ligação RDIS do **BinGO!** não pode ser conectada à Ethernet do seu computador ou Hubs, a ligação LANdo **BinGO!** não pode ser conectada à sua ligação RDIS.
- Para o cableamento, utilize unicamente o cabo fornecido juntamente. Se usar outro cabo, a BinTec Communications AG não se responsabiliza por danos daí decorrentes.
- Instale os cabos de maneira a não constituírem uma fonte de perigo (perigo de tropeçar) nem se danificarem.

- Não conecte nem desconecte os cabos de transmissão de dados se estiver a trovejar.

Utilização conforme com as especificações, Operação

- O**BinGO!** destina-se à utilização em escritórios. Enquanto Router multiprotocolo RDIS, o **BinGO!** estabelece as ligações RDIS em função da configuração do sistema. Para evitar taxas adicionais deve vigiar sempre o produto.
- O**BinGO!** corresponde às normas de segurança habituais relativas a dispositivos de informática para utilização em escritórios.
- O funcionamento conforme com as especificações IEC 950/EN 60950 do sistema só é garantido com a tampa da caixa montada (refrigeração, protecção contra incêndios, desparasitagem)
- A temperatura ambiente não pode ultrapassar 50˚C. Evite expor o aparelho à luz solar directa.
- Tenha o cuidado de não deixar entrar objectos (por ex. clipes) ou líquidos para o interior do aparelho (choque eléctrico, curto-circuito). Verifique se a refrigeração é suficiente.
- Em caso de emergência (por ex. caixa ou elemento de comando danificado, entrada de líquido ou de corpos estranhos), interrompa imediatamente a alimentação de corrente e recorra ao serviço de assistência técnica.

Limpeza e reparação

- O aparelho só pode ser aberto por pessoal especializado. Por isso, deixe as reparações do aparelho exclusivamente a cargo de um serviço de assistência técnica BinTec autorizado. Informe-se junto do seu agente para saber onde encontrar um ponto de assistência técnica. O utilizador pode colocar-se a si próprio em perigo caso abra o dispositivo sem qualquer autorização ou proceda a uma reparação imprópria (por ex. choque eléctrico). A abertura não autorizada do aparelho tem como consequência a perda da garantia e da responsabilidade daBinTec Communications AG.
- O aparelho nunca pode ser limpo a húmido. A infiltração de água pode constituir perigo para o utilizador (por ex. choque eléctrico) e danos de monta no aparelho.
- Nunca utilizar abrasivos, produtos de limpeza alcalinos, objectos afiados ou que risquem.

Instrucciones generales de seguridad

En los párrafos siguientes encontrará unas instrucciones de seguridad. Es imprescindible tener las mismas en cuenta a la hora de manejar su router.

Transporte y almacenamiento

- Transporte y almacene su **BinGO!** únicamente en su embalaje original o en otro embalaje adecuado que garantice su protección contra golpes y choques.

Colocación y puesta en servicio

- Antes de la colocación y puesta en servicio de **BinGO!**, observe las instrucciones acerca de las condiciones ambientales (ver “Datos técnicos”). Utilice una superficie firme y plana.
- Al trasladar el aparato desde un ambiente frío a la habitación prevista para su puesta en servicio puede formarse rocío tanto en el exterior como en el interior del aparato. Antes de ponerlo en marcha, espere hasta que su router se haya adaptado a la temperatura y esté absolutamente seco.
- Asegúrese de que la tensión nominal indicada en la placa de características coincide con la tensión de la red local. **BinGO!** únicamente debe ponerse en funcionamiento con el bloque de alimentación original de BinTec Communications (5 V DC). BinTec Communications AG no se hace responsable de los daños y perjuicios causados por el uso de otro tipo de bloque de alimentación.
- A la hora de cablear, respete el orden descrito en el manual. Cablee primero las conexiones LAN, RSDI y de serie, conecte la alimentación de energía eléctrica y encienda finalmente el **BinGO!**.
- Asegúrese del cableado correcto -y sobre todo del cableado de las conexiones LAN y RSDI- antes de poner **BinGO!** en servicio. La conexión RSDI de **BinGO!** no debe conectarse a la conexión Ethernet de su ordenador o hub, ni la conexión LAN de **BinGO!** a su conexión RSDI.
- Realice el cableado únicamente con los cables suministrados. Si utiliza cables distintos, BinTec Communications AG no asumirá la responsabilidad de los daños y perjuicios que puedan producirse.
- Coloque los cables de manera que no constituyan un peligro (tropezones) y no puedan ser deteriorados.

- No conecte ni desconecte líneas de transmisión de datos durante una tormenta

Utilización prevista, servicio

- **BinGO!** está previsto para su utilización en oficinas y despachos. Como router RSDI multiprotocolo, **BinGO!** crea conexiones RSDI en función a la configuración del sistema. Para evitar gastos telefónicos no deseados es imprescindible controlar el aparato
- **BinGO!** corresponde a las disposiciones de seguridad pertinentes para equipos informáticos utilizados en oficinas y despachos.
- El servicio previsto del sistema de acuerdo con IEC 950/EN 60950 queda únicamente garantizado si la tapa permanece montada en la caja (refrigeración, prevención de incendios, supresión de interferencias)
- La temperatura ambiental no debe superar los 50˚C. No exponga el aparato a la luz solar directa.
- Procure que ningún objeto (p. ej. clips) o líquido entre en el interior del aparato (descargas eléctricas , cortocircuitos) y que exista una refrigeración suficiente.
- En casos de emergencia (p. ej. caja o elemento de mando deteriorados, penetración de líquidos o de cuerpos extraños), interrumpa inmediatamente la alimentación de energía y avise al servicio técnico.

Limpieza y reparación

- El aparato debe ser abierto únicamente por personal técnico cualificado. Por lo tanto, realice las posibles reparaciones del aparato sólamente a través de un servicio técnico autorizado por BinTec. Su vendedor le informará de la dirección del servicio técnico. El abrir y reparar el aparato sin autorización puede conllevar un peligro considerable para el usuario (descargas eléctricas). El abrir de los aparatos sin autorización tiene como consecuencia la exoneración de la responsabilidad y de la garantía de BinTec Communications AG.
- En ningún caso, el aparato debe limpiarse en húmedo. Al penetrar agua, puede existir un peligro considerable para el usuario (p. ej., descargas eléctricas) y pueden producirse daños considerables en el aparato.
- No utilizar jamás productos abrasivos, detergentes alcalinos, ni instrumentos afilados o abrasivos.

Allmänna säkerhetsanvisningar på tyska

Nedan följer säkerhetsanvisningar som du måste ta hänsyn till när du använder din Router.

Transport och förvaring

- **BinGO!** får endast transporteras och förvaras i originalförpackningen eller i en annan lämplig förpackning som skyddar mot stötar och slag.

Installation och start

- Innan du installerar och börjar använda **BinGO!** bör du först läsa specifikationerna om miljökraven (se Tekniska Data). Använd ett fast och jämnt underlag.
- Om apparaten kommer utifrån och skall ställas upp inomhus kan det börja imma båda utvändigt och inuti apparaten. Vänta därför tills din nya Router har antagit rumstemperatur och är absolut torr innan du börjar använda den.
- Kontrollera att märkspänningen på typskylten stämmer överens med den lokala nätspänningen. **BinGO!** får endast användas tillsammans med original BinTec Communication nätenhet (5 V DC). BinTec Communications AG ansvarar inte för skador som kan hänföras till att en annan nätenhet har använts.
- Kablarna skall dras i den ordning som anges i handboken. Börja med kablarna till LAN-, ISDN- und de seriella anslutningarna, anslut sedan strömmen och starta **BinGO!**.
- Kontrollera att kabeldragningen har genomförts riktigt - särskilt ISDN- und LAN-kablarna - innan du börjar använda **BinGO!**. ISDN-anslutningen till **BinGO!** får inte anslutas till Ethernet-anslutningen på din dator eller på hubben och LAN-anslutningen till **BinGO!** får inte anslutas till din ISDN-anslutning.
- Använd endast bifogade kablar. Om du använder andra kablar kan BinTec Communications AG inte påta sig något ansvar för eventuella skador.
- Ledningarna skall dras så att de inte utgör någon risk (de får inte ligga så att man kan snubbla över dem) och inte kan skadas.
- Dataledningarna får varken anslutas eller lossas under ett oväder.

Normal användning, drift

- **BinGO!** är avsedd för att användas i kontorsmiljö. I egenskap av ISDN-multi-protokoll-router bygger **BinGO!** upp ISDN-linjer beroende på systemuppbyggnaden. För att undvika ofrivilliga avgifter bör du absolut övervaka produkten.
- **BinGO!** uppfyller kraven i gällande säkerhetsbestämmelser för IT-utrustning för kontor.
- För normal användning av systemet enligt IEC 950/EN 60950 måste locket vara monterat (kylning, brandskydd, gnistavstörning)
- Omgivningstemperaturen får inte vara högre än 50˚C. Undvik direkt solljus.
- Kontrollera att det inte kan hamna några föremål (t ex häftklammer) eller vätskor i apparaten (risk för kortslutning). Sörj för fullgod kylning.
- Bryt genast strömmen i nödsituationer (t ex om apparaten eller manöverelementen är trasiga eller om vätska eller främmande föremål har trängt in i den) och kontakta serviceavdelningen.

Rengöring och reparation

- Apparaten får endast öppnas av fackpersonal med motsvarande kompetens. Reparationer på apparaten får därför endast utföras av en av BinTec auktoriserad serviceverkstad. Var närmaste serviceverkstad finns kan du få reda på om du vänder dig till den affär där du köpt apparaten. Om apparaten öppnas av obehöriga eller repareras på felaktigt sätt kan allvarliga skador drabba den som använder apparaten (elektriska stötar). Om apparaten öppnas utan tillstånd gäller inte garanti- och ansvarsvillkoren för BinTec Communications AG längre.
- Apparaten får absolut inte våtrengöras. Om vatten tränger kan allvarliga skador drabba den som använder apparaten (t ex elektriska stötar) samt allvarliga maskinskador uppkomma.
- Apparaten får inte rengöras med skurpulver, alkaliska rengöringsmedel, skarpa medel eller medel som ger repor.

2 Všeobecné bezpečnostní pokyny

V následujících odstavcích najdete bezpečnostní pokyny, kterých musíte bezpodmínečně dbát při práci se svým routerem.

Doprava a uskladnění

- Dopravujte a skladujte **BinGO!** jen v originálním obalu nebo v jiném vhodném obalu, který zaručuje ochranu proti nárazu.

Postavení a uvedení do provozu

- Před postavením a uvedením **BinGO!** do provozu si povšimněte pokynů týkajících se podmínek prostředí (viz technické údaje). Pouijte pevnou a rovnou podloku.
- Je-li přístroj přenesen ze studeného prostředí do provozní místnosti, opotí se jak vnějšek přístroje, tak jeho vnitřek. Počkejte, ne váš router bude mít teplotu okolí a bude absolutně suchý, ne jej uvedete do provozu.
- Zkontrolujte, zda jmenovité napětí na typovém štítku síové části souhlasí s napětím v místní elektrické síti. **BinGO!** se smí provozovat jen s originální síovou přípojkou BinTec Communication. (5 V DC). BinTec Communications AG neručí za škody, které vzniknou pouitím jiného dílu pro napájení ze sítě.
- Při propojování kabelů dbejte na pořadí, jak je popsáno v příručce. Spojte nejprve LAN, ISDN a seriové přípojky, pak teprve zapojte napájení ze sítě a nakonec zapněte **BinGO!** .
- Zkontrolujte, jestli propojení, zvláště propojení ISDN a LAN, bylo provedeno správně, ne uvedete do provozu **BinGO!** Přípojka ISDN **BinGO!** nesmí být spojena s ethernetovou přípojkou vašeho počítače, přípojka LAN od - **BinGO!** s vaší přípojkou ISDN.
- Pro spojení pouijte výhradně přiloené kabely. V případě, e pouijete jiné kabely, nepřejímáBinTec Communications AG za nastalé škody ádnou zodpovědnost.
- Polote kabely tak, abyste se vyhnuli nebezpečí (např. zakopnutí) a aby se nepoškodily.
- Během bouřky nepřipojujte vedení přenosu dat ani je nevytahujte.

Uití k účelu, provoz

- **BinGO!** je určeno pro pouití v kancelářském prostředí. Jako multiprotokolový router ISDN buduje **BinGO!** v závislosti na systémové konfiiguraci spojení ISDN. Abyste se vyhnuli neádoucím poplatkům, měli byste mít výrobek bezpodmínečně pod dohledem.
- **BinGO!** odpovídá bezpečnostním předpisům pro zařízení informační techniky pro práci v kancelářském prostředí.
- Uití k patřičnému účelu podle IEC 950/EN 60950 systému je zaručeno pouze při nasazeném krytu skříně (chlazení, ochrana před poárem, odjiskření).
- Teplota prostředí by neměla překročit 50 °C. Vyhněte se přímému slunečnímu záření.
- Dbejte na to, aby se do vnitřku přístroje nedostaly ádné předměty (např. kancelářské svorky) nebo tekutiny (nebezpečí elektrického výboje, krátkého spojení). Dbejte na dostatečné chlazení.
- V případě tísně (např. poškozená skříň nebo ovládací prvek, vniknutí tekutiny nebo cizích těles) okamitě přerušte přívod proudu a zavolejte servis.

Čištění a opravy

- Přístroj smí otvírat jen školený odborný personál. Dávejte proto provádět opravy přístroje jen do autorizovaného servisu firmy BinTec. Kde tento servis je, se dozvíte od svého obchodníka. Při neoprávněném otevření a neodborných opravách se uivatel může vystavit značným nebezpečím (např. úderu proudu). Nedovolené otevření přístroje má za následek zánik záruky a ručení firmy BinTec Communications AG .
- Přístroj se v ádném případě nesmí čistit mokrým předmětem. Vniknoucí voda vystavuje uivatele vánému nebezpečí (např. úderu proudu) a způsobí váné poškození přístroje.
- Nikdy nepouívejte čisticí prášky, alkalická čistidla, ostré předměty nebo prostředky k drhnutí.

Genel güvenlik bilgileri türkçe

Müteakip bölümlerde router'inizin kullanýrken mutlaka dikkat etmeniz gereken genel güvenlik bilgilerini bulabilirsiniz.

Transport ve Depolama

- **BinGO!** yalnýzca orijinal ambalajý içinde veya çarpmaya ve darbeye karþý koruma saðlayan diðer bir ambalaj içinde taþýnmalý ve depolanmalýdýr.

Kurulmasý ve Çalýþtýrýlmasý

- **BinGO!** kurulup ve çalýþtýrýlmadan önce çevre koþullarý hakkýndaki bilgiler dikkate alýnmalýdýr (Teknik özellikler). Saðlam duran ve düz bir altlýk kullanýnýz.
- Eðer cihaz soðuk bir ortamdan iþletim odasýna getirilirse cihazýn dýþýnda ve içinde nem oluþabilir. Bu durumda router'inizi çalýþtýrmadan önce bulunduðu ortamdaki ýsýya adapte olmasýný ve tamamen kurumasýný bekleyiniz.
- Trafonun tip etiketindeki anma gerilimin yerel þebeke gerilimi ile eþit deðerde olup olmadýðýný kontrol edin. **BinGO!** yalnýzca orijinal BinTec Communications fiþli trafo (5 V DC) ile iþletilmelidir. BinTec Communications AG baþka bir trafo ile kullanýmdan kaynaklanan hasarlar için sorumluluk üstlenmez.
- Kablo baðlantýlarýný yaparken el kitabinda açýklanan sýralamaya göre çalýþýn. Ýlkönce LAN-, ISDN- ve seri baðlantý yuvalarýna olan kablo baglantýsýný tamamlayýn, sonra elektrik beslemesini baðlayýn, ve son olarak **BinGO!** 'yu çalýþtýrýn.
- **BinGO!** çalýþtýrmadan önce kablo baðlantýlarýnýn – özellikle ISDN- ve LAN kablo baðlantýlarý – doðru olup olmadýðýný kontrol edin. **BinGO!** 'nun ISDN baðlantý yuvasý bilgisayarýnýzýn ve hub'ýnýzýn Ethernet baðlantýsý ile, **BinGO!** 'nun LAN-baðlantýsý sizin ISDN baðlantýnýz ile birleþtirilmemelidir.
- Kablo baðlantýlarý için yalnýzca cihazla beraber gönderilen kablolarý kullanýn. Eðer baþka kablo kullanýrsanýz BinTec Communications AG meydana gelen hasarlar için sorumluluk üstlenmez.
- Kablolarý döþerken tehlike kaynaðý (tökezleme tehlikesi) yaratmamaya özen gösterin ve kablolarý hasar görmeyecek þekilde döþeyin.

- Veri aktarým kablolarýný kötü hava esnasýnda (yaðmur, þimþek vs.) baðlamayýn veya çýkarmayýn.

Amacýna uygun kullaným, Ýþletim

- **BinGO!** yalnýzca büro ortamýnda kulanýlmak üzere tasarlanmýþtýr. ISDN-Multi-Protokoll-Router'i olarak **BinGO!** sistem konfigürasyonuna baðýmlý olarak ISDN-baðlantýlarýný kurar. Ýstekdýþý ücretlerin önlenmesi için ürün mutlaka kontrol edilmelidir.
- **BinGO!** büro ortamýnda kullanýlan bilgi teknolojisi donanýmlarý ile ilgili güvenlik yönetmeliklerine uygundur.
- Sistemin IEC 950/EN 60950'ye göre kurallara uygun iþletimi, yalnýzca cihaz kasasýnýn kapaðý monte edili ise saðlanýr (soðutma, yangýn koruma, parazit giderme)
- Çevre ýsýsý 50°C üstüne çýkmamalýdýr. Cihazý güneþ ýþýnlarýndan koruyun.
- Cihazýn içine yabancý cisimlerin (örnegýn ataç) veya sývýlarýn girmesini önleyin (elektrik çarpmasý, kýsa devre). Cihazýn yeterli derecede soðutulmasýna dikkat edin.
- Acil durumlarda (örneðin hasar görmüþ cihaz kasasý veya kumandaelemaný, sývý veya yabancý cisimlerin cihaz içine girmesi) derhal elektrik beslemesini kapatýn ve servise haber verin.

Temizlik ve Tamir

- Cihazýn yalnýzca eðitilmiþ kalifiye personel tarafýndan açýlmasýna izin verilmiþtir. Bu nedenle cihazdaki tamir iþlerinin yalnýzca BinTec yetkili servisi tarafýndan yapýlmasýný saðlayýn. Servisin adresini cihazý satýn aldýgýnýz satýcýdan öðrenebilirsiniz. Cihazýn izinsiz açýlmasýndan ve bilgisizce yapýlan tamirlerden dolayý kullanýcý için ciddi tehlikeler oluþabilir (örneðin elektrik çarpmasý). Cihazlarýn izin olmadan açýlmasý sonucunda BinTec Communications AG firmasýnýn garanti ve sorumluluk yükümlülüðü ortadan kalkar.
- Cihazýn suyla temizlenmesi kesinlikle yasaktýr. Cihazýn içine su girmesi sayesinde kullanýcý için ciddi tehlikeler oluþabilir (örneðin elektrik çarpmasý) ve cihazda ciddi hasarlar meydana gelebilir.
- Kesinlikle alkalik temizlik maddesi, keskin veya aþýndýrýcý yardýmcý madde kullanmayýnýz.

Általános biztonsági útmutató

A következõ fejezetekben olyan biztonsági útmutatásokat talál, amelyeket routere használata során feltétlenül figyelembe kell vegyen.

Szállítás és tárolás

- A **BinGO!** csak az eredeti csomagolásban szállítandó és tárolandó, vagy egy másik arra alkalmas csomagolásban, amely lökések és ütések ellen védelmet biztosít.

Felállítás és üzembehelyezés

- A **BinGO!** felállítása és üzemeltetése elõtt vegye figyelembe a környezeti feltételekre vonatkozó útmutatásokat (lásd a mûszaki adatoknál). Használjon szilárd és sík alapot.
- Amennyiben a berendezést hideg környezetbõl szállítják be az üzemi helyiségbe, akkor fennáll a harmatképzõdés lehetõsége úgy a készülék külsején, mint pedig annak belsejében. Mielõtt üzembe helyezné várjon addig, amíg routere hõmérséklete alkalmazkodott a környezetéhez és teljesen kiszáradt.
- Ellenõrizze, hogy a tápegység típustábláján megadott névleges feszültség megegyezik-e a helyi hálózati feszültséggel. A **BinGO!** csak az eredeti BinTec Communications dugaszolható tápegységgel (5 V DC) üzemeltethetõ. A BinTec Communications AG nem felel olyan károkért, amelyek egy más típusú dugaszolható tápegység használata révén keletkeztek.
- A kábelezéskor vegye figyelembe a kézikönyvben megadott sorrendet. Elõször kábelezze be a LAN-, ISDN- és soros csatlakozásokat, ezek után csatlakoztassa az áramellátást, végezetül pedig kapcsolja be a **BinGO!** -t.
- Ellenõrizze, hogy a kábelezés - különösen az ISDN- és LAN-kábelezés - helyesen lett-e kivitelezve, mielõtt a **BinGO!** üzembehelyezése megtörténne. A **BinGO!** ISDN csatlakozóját nem szabad az Ön számítógépének vagy hálózati meghajtójának Ethernet csatlakozójával, a **BinGO!** LAN-csatlakozását pedig tilos az Ön ISDN-csatlakozójával összekötni.
- A kábelezéshez csak a mellékelt kábeleket szabad felhasználni. Amennyiben más kábeleket alkalmaz, úgy a BinTec Communications AG az esetlegesen keletkezõ károkért a felelõsséget nem vállalja.
- Fektesse le úgy a kábeleket, hogy azok ne lehessenek veszélyek forrásai (botlásveszély) és azokban kár sem keletkezhessen.

- Viharos idõben ne csatlakoztasson adatátviteli kábeleket és ne is húzza ki azokat.

Rendeltetés szerinti használat, üzemeltetés

- **BinGO!** irodai jellegû környezetben történõ használatra készült. Mint ISDN-multi-protokoll-router **BinGO!** a rendszer konfigurációjától függõen ISDN-kapcsolatokat épít fel. Az akaratlan költségek elkerülése végett a termék feltétlenül felügyeletre szorul.
- **BinGO!** megfelel az idevágó - irodai környezetben való használatra alkalmas információtechnikai berendezésekre vonatkozó - biztonsági elõírásoknak.
- A rendszer rendeltetésszerû használata IEC 950/EN 60950 szerint csak a készülék házának felszerelt tetõzete esetében biztosított (hûtés, tûzvédelem, zavarmentesítés).
- A környezeti hõmérséklet az 50˚C értéket ne haladja meg. A közvetlen napsugárzás elkerülendõ.
- Legyen figyelemmel arra, hogy a készülék belsejébe ne kerülhessenek be tárgyak (pld. gémkapocs) vagy folyadékok (áramütés, rövidzárlat). Figyeljen oda a kielégítõ hûtésre.
- Vészhelyzetben (pld. sérült készülékház vagy kezelõelem esetében, vagy amennyiben folyadék vagy idegen test kerülne bele) azonnal szakítsa meg az áramellátást és értesítse a szervízt.

Tisztítás és javítás

- A készüléket csak arra kioktatott szakszemélyzet nyithatja fel. Ezért a készüléken esedékes javításokat csak egy a BinTec által erre feljogosított szervízzel végeztesse el. Hogy ezen szervíz hol található, azt Ön a kereskedõjétõl tudhatja meg. A készülék jogtalan felnyitása és a helytelen javítás révén a felhasználó számára jelentõs veszélyforrások keletkezhetnek (pld. áramütés). A készülékek engedély nélkül történõ felnyitása a BinTec Communications AG garanciális és felelõsségvállalási kötelezettségének megszûnését vonja maga után.
- A készüléket semmi esetre sem szabad nedvesen tisztítani. A víz behatolása a felhasználó számára jelentõs veszélyt jelent (pld. áramütés) és a készülékben is komoly károk keletkezhetnek.

- Sohasem szabad súrolószereket, lúgos tisztítószereket, éles vagy karcoló segédeszközöket alkalmazni.

13 Allgemeine Sicherheitshinweise in 15 verschiedenen Sprachen

100Base-T Twisted Pair-Anschluß, Fast Ethernet. Netzwerkanschluß für 100 MBit-Netze.

10Base-T Twisted Pair-Anschluß. Netzwerkanschluß für 10 MBit-Netze mit dem Steckertyp ➤➤ **RJ45**.

10Base-2 Thin Ethernet-Anschluß. Netzwerkanschluß für 10 MBit-Netze mit dem Stekkertyp BNC. Zum Anschluß von Geräten mit BNC-Buchsen werden T-Verbindungsstücke eingesetzt.

1TR6 Im deutschen ISDN verwendetes D-Kanal-Protokoll. Heute gängigeres Protokoll ist das ➤➤ **DSS1**.

a/b Standardschnittstelle für analoge Endgeräte (Telefon, Telefax Gruppe 2/3, analoge Modems). Nur bei BinTec-Routern mit intergrierter ➤➤ **PABX**.

ARP Address Resolution Protocol

ARP gehört zur ➤➤ **TCP/IP-Protokollfamilie**. ARP löst IP-Adressen in zugehörige ➤➤ **MAC-Adressen** auf.

asynchron Übertragungsverfahren, bei dem die Zeitabstände zwischen übertragenen Zeichen unterschiedlich lang sein können. Dadurch können Geräte miteinander kommunizieren, die nicht in gleichen Zeittakten arbeiten. Anfang und Ende der übertragenen Zeichen müssen durch Start- und Stop-Bits gekennzeichnet sein – im Gegensatz zu ➤➤ **synchron**.

B-Kanal Basiskanal eines ➤➤ **ISDN-Basisanschlusses** bzw. ➤➤ **Primärmultiplexanschlusses** zur Übertragung von Nutzinformationen (Sprache, Daten). Ein ISDN-Basisanschluß besitzt zwei B-Kanäle und einen ➤➤ **D-Kanal**. Ein B-Kanal hat eine Datenübertragungsrate von 64 kbit/s.

Durch ➤➤ **Kanalbündelung** kann mit **BinGO!** die Datenübertragungsrate bei einem ISDN-Basisanschluß auf bis zu 128 kbit/s gesteigert werden.

BootP Bootstrap Protocol

Basiert auf dem ➤➤ **UDP** bzw. ➤➤ **IP-Protokoll**. Dient zur automatischen Vergabe einer ➤➤ **IP-Adresse**. In den DIME Tools ist ein BootP-Server enthalten, den Sie auf Ihrem PC starten können, um dem noch unkonfigurierten Router eine IP-Adresse zuzuweisen.

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

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

Einige BinTec-Router können im Bridging-Modus betrieben werden.

Broadcast Broadcasts sind Rundrufe (Datenpakete), die an alle im Netz angeschlossenen Geräte gesendet werden, um Informationen im Netz auszutauschen. Normalerweise gibt es im Netz eine bestimmte Adresse (Broadcast-Adresse), die es allen Geräten ermöglicht, eine Nachricht als Broadcast zu interpretieren.

Bus Ein Medium zur Datenübertragung für alle Geräte im Netz. Die Daten werden über den gesamten Bus verbreitet und von allen Geräten am Bus empfangen.

Called Party's Number Nummer des Angerufenen.

Calling Party's Number Nummer des Anrufers.

CAPI Common ISDN Application Programming Interface

1989 standardisierte Software-Schnittstelle, die es Anwendungsprogrammen ermöglicht, auf ISDN-Hardware vom Rechner aus zuzugreifen. Die meisten ISDN-spezifischen Software-Lösungen (Kommunikationsprogramme wie RVS-COM Lite) arbeiten mit der CAPI-Schnittstelle. Über solche Kommunikationsprogramme können Sie z. B. von Ihrem Rechner aus über das ISDN Faxe verschicken und empfangen oder Daten übertragen. Siehe auch ➤➤ **Remote-CAPI**.

CCITT Commite Consultatif International Telegraphique et Telephonique

Ehemals ein Gremium der ➤➤ **ITU**, das Empfehlungen im Bereich Fernmeldewesen, öffentliche Telefon-/Daten-Netze und Schnittstellen zur Datenübertragung verabschiedet hat.

CHAP Challenge-Handshake Authentication Protocol

Sicherheitsmechanismus beim Verbindungsaufbau mit einem ➤➤ **WAN-Partner** über ➤➤ **PPP**. Dieses Protokoll dient der Überprüfung des WAN-Partnernamens und des Paßwortes, die für den WAN-Partner definiert sind. Stimmen Partnername und Paßwort auf beiden Seiten nicht überein, wird keine Verbindung aufgebaut. Benutzername und Paßwort werden bei CHAP verschlüsselt, bevor sie zum Partner übertragen werden – im Gegensatz zu ➤➤ **PAP**.

CLID Calling Line Identification (Rufnummernüberprüfung)

Sicherheitsmechanismus beim Verbindungsaufbau mit einem ➤➤ **WAN-Partner**. Ein Anrufer wird anhand seiner ISDN-Rufnummer erkannt bevor die Verbindung aufgebaut wird. Stimmt die Rufnummer nicht mit der Rufnummer überein, die Sie für einen WAN-Partner festgelegt haben, wird keine Verbindung aufgebaut.

Client Ein Client nutzt die vom einem ➤➤ **Server** angebotenen Dienste. Clients sind in der Regel Arbeitsplatzrechner.

Datagramm Ein in sich abgeschlossenes ➤➤ **Datenpaket**, das mit einem Minimum an Protokoll-Overhead im Netz weitergeleitet wird – ohne Quittierungsmechanismus.

Datenkompression Methode, um übertragene Datenmengen zu verringern. Bei gleicher Übertragungsdauer kann so der Durchsatz erhöht werden. Bekannte Verfahren sind z. B. ➤➤ **V.42bis**, ➤➤ **STAC**, ➤➤ **VJHC**, ➤➤ **MPPC**.

Datenpaket Ein Datenpaket dient der Übermittlung von Informationen. Jedes Datenpaket enthält eine vorgeschriebene Anzahl von Zeichen (Informationen und Steuerzeichen).

DHCP Dynamic Host Configuration Protocol

Protokoll von Microsoft zur dynamischen Vergabe von ➤➤ **IP-Adressen**. Ein DHCP-Server vergibt an jeden ➤➤ **Client** im Netzwerk eine IP-Adresse aus einem definierten Adreß-Pool, der vom System-Administrator festgelegt wird. Voraussetzung: ➤➤ **TCP/IP** ist bei den Clients so konfiguriert, daß die Clients ihre IP-Adresse vom Server anfordern. **BinGO!** kann als DHCP-Server eingesetzt werden.

DIME Desktop Internetworking Management Environment

Die DIME Tools sind eine Sammlung von Werkzeugen zur Konfiguration und Überwachung von Routern über Windows-Applikationen. Wird mit jedem BinTec-Router kostenlos mitgelierfert.

DIME Browser Windows-Applikation (ähnlich dem Windows-Explorer), die SNMP-Kommandos benutzt, um die Einstellungen von **BinGO!** abzufragen und vorzunehmen.

D-Kanal Steuerkanal eines ➤➤ **ISDN-Basisanschlusses** bzw. ➤➤ **Primärmultiplexanschlusses**. Der der D-Kanal hat eine Datenübertragungsrate von 16 kbit/s. Außer dem D-Kanal besitzt jeder ISDN-Basisanschluß zwei ➤➤ **B-Kanäle**.

DNS Domain Name System

Jedes Gerät wird in einem ➤➤ **TCP/IP-Netz** normalerweise durch seine ➤➤ **IP-Adresse** angesprochen. Da in Netzwerken oft ➤➤ **Hostnamen** benutzt werden, um verschiedene Geräte anzusprechen, muß die zugehörige IP-Adresse bekanntgegeben werden. Diese Aufgabe übernimmt z. B. ein DNS-Server. Er löst die Hostnamen in IP-Adressen auf. Eine Namensauflösung kann alternativ auch über die sogenannte HOSTS-Datei erfolgen, die auf jedem Rechner zur Verfügung steht.

Domäne Ein Domäne ist ein logischer Zusammenschluß von Geräten in einem Netzwerk. Im ➤➤ **Internet** Teil einer Namenshierarchie (z. B. bintec.de).

DSS1 Digital Subscriber Signalling System

Im Euro-ISDN verwendetes, gängiges D-Kanal-Protokoll.

EAZ Endgeräteauswahlziffer

Gibt es nur im ➤➤ **1TR6** und bezeichnet die letzte Ziffer einer Rufnummer. Wird verwendet, um verschiedene Endgeräte (z. B. Fax) anzuwählen, die am ISDN-Basisanschluß angeschlossen sind. Dies geschieht durch Anhängen einer Ziffer zwischen 0 und 9 an die eigentliche ISDN-Rufnummer. Beim Euro-ISDN (DSS1) wird statt der EAZ die komplette Rufnummer, ➤➤ **MSN**, übertragen.

Encapsulation Enkapsulierung von ➤➤ **Datenpaketen** in ein bestimmtes Protokoll, um die Datenpakete über ein Netzwerk zu übertragen, das den ursprünglichen Protokolltyp nicht direkt unterstützt (z. B. NetBIOS über TCP/IP).

Encryption Bezeichnet die Verschlüsselung von Daten, z. B. ➤➤ **MPPE**.

Ethernet Ein lokales Netzwerk, das alle Geräte im Netz (Rechner, Drucker, etc.) über ein Twisted Pair- oder Koaxialkabel verbindet.

Festverbindung Standleitung (leased line)

Feste Verbindung zu einem Teilnehmer. Im Gegensatz zu einer ➤➤ **Wählverbindung** werden weder eine Rufnummer, noch Verbindungsauf- und -abbau benötigt.

Filter Eine Regel, die eine Anzahl von Datenpaketen definiert, die vom Router übertragen bzw. nicht übertragen werden sollen.

Firewall Bezeichnet die Summe der Schutzmechanismen für das lokale Netzwerk gegen Zugriffe von außen. Mit **BinGO!** stehen Schutzmechanismen wir ➤➤ **NAT**, ➤➤ **CLID**, ➤➤ **PAP/CHAP**, Accesslisten etc. zur Verfügung.

FTP File Transfer Protocol

TCP/IP-Protokoll zum Übertragen von Daten zwischen verschiedenen Rechnern.

Gateway Aus-/Einfahrt, Übergangspunkt

Komponente im lokalen Netzwerk, die Zugang zu anderen Netzwerken bietet, ermöglicht auch Netzübergänge zwischen unterschiedlichen Netzen, z. B. ➤➤ **LAN** und ➤➤ **WAN**.

Hostname Bezeichnet in ➤➤ **IP**-Netzen einen Namen, der als Ersatz einer zugehörigen ➤➤ **IP-Adresse** benutzt wird. Ein Hostname besteht aus einer ASCII-Zeichenfolge, die den Host eindeutig kennzeichnet.

Hub Netzwerkkomponente, mit der mehrere Netzwerkkomponenten zu einem lokalen Netz zusammengeschlossen werden (sternförmig).

Internet Das Internet besteht aus einer Reihe von regionalen, lokalen und Universitätsnetzen. Für Datenübertragung im Internet wird das Protokoll ➤➤ **IP** verwendet.

IP Internet Protocol

Gehört zur Protokollfamilie ➤➤ **TCP/IP** zum Verbinden von Wide Area Networks (➤➤ **WANs**).

IP-Adresse In einem IP-Netzwerk der erste Teil der Adresse, mit der sich ein Gerät im Netzwerk identifiziert, z. B. 192.168.1.254. Siehe auch ➤➤ **Netzmaske**.

ISDN Integrated Services Digital Network

Das ISDN ist ein digitales Netz, das die Übertragung von Sprache und Daten ermöglicht. Für das ISDN gibt es zwei mögliche Teilnehmeranschlüsse, der ➤➤ **ISDN-Basisanschluß** und der ➤➤ **Primärmultiplexanschluß**. ISDN ist ein internationaler Standard. Für die Protokolle des ISDN hingegen gibt es eine Vielzahl von Varianten.

ISDN-Basisanschluß Teilnehmeranschluß beim ISDN. Der Basisanschluß besteht aus zwei ➤➤ **B-Kanälen** und einem ➤➤ **D-Kanal**. Außer dem Basisanschluß gibt es noch den ➤➤ **Primärmultiplexanschluß**.

Die Schnittstelle zum Teilnehmer wird über den sog. ➤➤ **S_0-Bus** geschaffen.

ISO International Standardization Organization

Internationale Organisation zur Entwicklung weltweiter Normen, z. B. ➤➤ **OSI-Modell**.

ISP Internet Service Provider

Ermöglicht Firmen oder Privatpersonen den Zugriff auf das Internet.

IP-Adresse IP = Internet Protocol

IPX/SPX Internet Packet Exchange/Sequenced Packet Exchanged

Protokollfamilie von Novell zur Übertragung von Daten in einem Netzwerk. Die beiden Bestandteile dieser Protokollfamilie sind IPX (Schicht 3 des OSI-Modells) und SPX (Schicht 4 des OSI-Modells).

ISDN-Login Funktion von **BinGO!**. Über ISDN-Login ist **BinGO!** fernkonfigurier- und wartbar. ISDN-Login funktioniert bereits bei Routern im Auslieferungszustand, sobald sie mit einem ISDN-Anschluß verbunden und so über eine Rufnummer erreichbar sind.

ITU International Telecommunication Union

Internationale Organisation, die den Aufbau und den Betrieb von Telekommunikationsnetzen/-diensten koordiniert.

Kanalbündelung Funktion von **BinGO!**. Kanalbündelung ist eine Methode, den Datendurchsatz zu erhöhen. Indem (dynamisch = bei Bedarf oder statisch = immer) ein zweiter ➤➤ **B-Kanal** zur Datenübertragung hinzugeschaltet wird, verdoppelt sich der Durchsatz.

LAN Local Area Network (Lokales Netzwerk)

Räumlich eng begrenztes Netzwerk, das sich unter Kontrolle eines Besitzers befindet. Meist innerhalb eines Gebäudes/Firmensitzes.

MAC-Adresse Jedes Gerät im Netz ist über eine feste Hardware-Adresse (MAC-Adresse) definiert. Die Netzwerkkarte eines Geräts bestimmt diese weltweit eindeutige Adresse.

MIB Management Information Base

MIB ist eine Datenbank, die alle im Netz angeschlossenen managebaren Geräte und Funktionen beschreibt. Jede MIB (so auch die BinTec MIB) enthält hersteller-spezifische Objekte. ➤➤ **SNMP** setzt auf MIB auf.

Modem Modulator/Demodulator

Ein elektronisches Gerät. Wird verwendet, um digitale Signale in (analoge) Tonfrequenzsignale umzuwandeln und umgekehrt, so daß die Daten auf einer analogen Leitung übertragen werden können.

MPPC Microsoft Point-to-Point Compression

Verfahren zur Datenkompression.

MPPE Verfahren zur Datenverschlüsselung.

MSN Multiple Subscriber Number

Mehrfachnummer für einen ISDN-Basisanschluß im Euro-ISDN. Die MSN ist die Rufnummer, die im Euro-ISDN das gezielte Ansprechen eines Endgerätes am ➤➤ **S_0-Bus** erlaubt. Eine MSN hat bis zu acht Stellen, z. B. 49 911 7654321, wobei die 7654321 der MSN entspricht.

In der Regel erhält man in Deutschland mit dem ISDN-Basisanschluß drei solcher MSNs.

Multiprotokollrouter ➤➤ **Router**, der mehrere Protokolle routen kann, z. B. ➤➤ **IP**, ➤➤ **IPX** etc.

NAT Network Address Translation

Sicherheitsmechanismus von **BinGO!**. Über NAT wird ein komplettes Netzwerk nach außen hin verborgen. Die IP-Adressen aller Geräte im eigenen Netz bleiben geheim, nur eine einzige IP-Adresse wird für Verbindungen nach außen bekanntgegeben.

NetBIOS Network Basic Input Output System

Programmierschnittstelle, die Netzwerkoperationen auf einem PC aktiviert. Kommandoset zum Übertragen und Senden von Daten zu anderen Windows-Rechnern im Netzwerk.

Netzadresse Eine Netzadresse bezeichnet die Adresse eines gesamten lokalen Netzwerks.

Netzmaske In einem IP-Netzwerk der zweite Teil der Adresse, mit der sich ein Gerät im Netzwerk identifiziert, z. B. 255.255.255.0. Siehe auch ➤➤ **IP-Adresse**.

NTBA Network Termination for Basic Access.

Ein NTBA-Adapter ist das Netzabschlußgerät eines ➤➤ **ISDN-Basisanschlusses**, den Sie in Deutschland bei der Deutschen Telekom AG erhalten. Er schafft den Anschluß des privaten Netzes (➤➤ **S_0-Bus**) an das öffentliche ISDN-Netz. Es entspricht dem Verteilerkästchen (TAE-Dose) beim analogen Telefon-Anschluß.

OSI-Modell OSI = Open System Interconnection (offene Kommunikationssysteme)

Referenzmodell der ➤➤ **ISO** für Netzwerke. Definiert Schnittstellen-Standards zwischen Computerherstellern in den Bereichen Software- und Hardwareanforderungen.

OSPF Open Shortest Path First

Routing-Protokoll, das in Netzwerken verwendet wird, um Informationen (Routing-Tabellen) zwischen ➤➤ **Routern** auszutauschen.

PABX Private Automatic Branch Exchange (Nebenstellenanlage)

ISDN ➤➤ **TK-Anlage** mit ➤➤ **S_0-Schnittstelle** und ➤➤ **1TR6** bzw. anderen herstellerspezifischen ➤➤ **D-Kanal-Protokollen** auf der Teilnehmerseite.

Nebenstellenanlagen ermöglichen interne Verbindungen zwischen den Anschlüssen der TK-Anlage, ohne daß dabei auf Telefonanbieter zugegriffen werden muß. Nicht alle BinTec-Router enthalten eine Nebenstellenanlage.

PAP Password Authentication Protocol

Authentisierungsverfahren für Verbindungen über ➤➤ **PPP**. Funktioniert wie ➤➤ **CHAP**, außer daß Benutzername und Paßwort nicht verschlüsselt werden, bevor sie zum Partner übertragen werden.

Ping Packet Internet Groper

Befehl, über den man die Entfernung entfernter Netzwerkkomponenten ermitteln kann. Ping wird auch für Testzwecke verwendet, um festzustellen, ob das entfernte Gerät überhaupt erreicht werden kann.

Port Ein-/Ausgang

Anhand der Port-Nummer wird entschieden, an welche Dienste (Telnet, WWW) ein ankommendes Datepaket weitergeleitet wird.

PPP Point-to-Point Protocol

Protokollfamilie zur Aushandlung der Verbindungsparameter einer ➤➤ **Punkt-zu-Punkt-Verbindung**. PPP wird bei der Kopplung von lokalen Netzen über das ➤➤ **WAN** verwendet. Multiprotokoll-Pakete werden für den Versand in ein einheitliches Format gekapselt (➤➤ **Encapsulation**). Der Verbindungsaufbau enthält eine Reihe weiterer Bestandteile und Teilprotokolle, wie Authentisierungsmechanismenen über ➤➤ **PAP/CHAP**.

PPP Authentsierung Sicherheitsmechanismus. Authentisierung durch ein Paßwort im ➤➤ **PPP**.

Primärmultiplexanschluß Teilnehmeranschluß beim ISDN. Der Primärmultiplexanschluß besteht aus einem D-Kanal und 30 B-Kanälen (Europa). (In Amerika: 23 B-Kanäle und ein D-Kanal.) Außer dem Primärmultiplexanschluß gibt es noch den ➤➤ **ISDN-Basisanschluß**.

Protokoll Protokolle werden verwendet, um Art und Weise eines Informationsaustausches zwischen zwei Systemen zu definieren. Protokolle steuern und regeln den Ablauf einer Datenkommunikation auf verschiedenen Ebenen (Decodierung, Adressierung, Wegwahl im Netz, Kontrollmechanismen, etc.).

Proxy ARP ARP = Address Resolution Protocol

Verfahren, mit dem für einen Host, dessen ➤➤ **IP-Adresse** bekannt ist, die zugehörige ➤➤ **MAC-Adresse** ermittelt wird.

Punkt-zu-Mehrpunkt Point-to-Multipoint

Merkmal einer Verbindung, die zwischen drei oder mehreren Datenstationen festgeschaltet oder über Vermittlungseinrichtungen hergestellt ist.

Punkt-zu-Punkt Point-to-Point

Merkmal einer Verbindung zwischen genau zwei Datenstationen. Die Verbindung kann festgeschaltet oder über Vermittlungseinrichtungen geführt sein.

Remote Entfernt, nicht lokal.

Wenn sich eine Gegenstation nicht im eigenen lokalen Netzwerk (LAN) befindet, sondern in einem anderen (remote) LAN, spricht man von Remote.

Dieses LAN muß dazu über eine WAN-Verbindung (über **BinGO!**) mit dem lokalen LAN verbunden sein.

Remote Access Nicht lokaler Zugriff, siehe ➤➤ **Remote**.

Remote-CAPI BinTec-eigene Schnittelle für ➤➤ **CAPI**.

Die Remote-CAPI-Schnittstelle ermöglicht allen Teilnehmern eines Netzes, CAPI-Dienste nutzen, dabei aber über **BinGO!** auf einen einzigen ISDN-Anschluß zuzugreifen. Voraussetzung ist, daß alle Teilnehmer eine geeignete Anwendungssoftware installiert haben, die die CAPI-Schnittstelle unterstützt. Diese genormte Schnittstelle wird von den meisten Kommunikationsanwendungen verwendet. Im Lieferumfang von **BinGO!** ist eine entsprechende Software (RVS-COM Lite) enthalten.

Die CAPI-Schnittstelle von BinTec ist als Dualmode-CAPI realisiert. Es können parallel CAPI 1.1- und 2.0-Anwendungen auf die ISDN-Ressourcen zugreifen. Somit können neben alten auf CAPI 1.1 basierenden Anwendungen, parallel im Netz oder auf dem gleichen Rechner, neue CAPI 2.0-Anwendungen betrieben werden.

RIP Routing Information Protocol

Routing-Protokoll, das in Netzwerken verwendet wird, um Informationen (Routing-Tabellen) zwischen ➤➤ **Routern** auszutauschen.

RJ45 Stecker bzw. Buchse für maximal acht Adern. Anschluß für digitale Endgeräte.

Router Geräte, die unterschiedliche Netze auf der Ebene 3 des ➤➤ **OSI-Modells** verbinden und Informationen von einem Netz in das andere weiterleiten (routen).

Router sind in der Lage, die verwendeten Informationsblöcke zu erkennen und Adressen auszuwerten (im Gegensatz zu einer ➤➤ **Bridge**, die Protokoll-transparent arbeitet). Anhand von Routing-Tabellen werden die besten Wege (Routen) von einer Stelle zur anderen festgelegt. Um die Routing-Tabellen auf dem Laufenden zu halten, tauschen die Router untereinander Informationen über Routing-Protokolle aus (z.B. ➤➤ **OSPF**, ➤➤ **RIP**).

Moderne Router wie **BinGO!** sind ➤➤ **Multiprotokollrouter** und dadurch in der Lage, mehrer Protokolle zu routen (z B. IP und IPX).

S_0-Anschluß Siehe ➤➤ **ISDN-Basisanschluß**.

S_0-Bus Sämtliche ISDN-Anschlußdosen und der ➤➤ **NTBA** beim ISDN-Mehrgeräte-anschluß. Jeder S_0-Bus besteht aus einem vieradrigen Kabel. Die Leitungen/ Kabel übertragen die digitalen ISDN-Signale. Hinter der letzten ISDN-Anschlußdose wird der S_0-Bus mit einem Abschlußwiderstand terminiert. Der S_0 beginnt beim NTBA und kann bis zu 150 m lang sein. Es lassen sich beliebige ISDN-Geräte daran betreiben. Gleichzeitig können allerdings immer nur zwei Geräte den S_0 verwenden, da nur zwei ➤➤ **B-Kanäle** zur Verfügung stehen.

S_2M-Anschluß Siehe ➤➤ **Primärmultiplexanschluß**.

Server Ein Server bietet Dienste an, die von ➤➤ **Clients** in Anspruch genommen werden. Oft versteht man unter Server einen bestimmten Rechner im LAN, z. B. DHCP-Server.

Bei einer Client-Server-Architektur ist ein Server der Softwareteil, der Dienste im Auftrag seines Clients ausführt, z. B. ➤➤ **TFTP-Server**. Dabei handelt es sich nicht unbedingt um einen bestimmten Server-Rechner.

Setup Tool Menügesteuertes Tool zur Konfiguration von **BinGO!**. Das Setup Tool kann verwendet werden, sobald ein Zugang zum Router (seriell, ➤➤ **ISDN-Login**, ➤➤ **LAN**) besteht.

Shorthold Bezeichnet die definierte Zeit, wann eine Verbindung abgebaut wird, wenn keine Daten mehr übertragen werden. Der Shorthold läßt sich statisch (feste Zeit) und dynamisch (in Abhängigkeit von Gebühreninformationen) einrichten.

SNMP Simple Network Management Protocol

Ein Protokoll in der ➤➤ **TCP/IP-Protokollfamilie** zum Transport von Managementinformationen über Netzwerkkomponenten. Zu den Bestandteilen eines jeden SNMP-Managementsystems zählt u. a. eine ➤➤ **MIB**. Über SNMP sind verschiedene Netzwerkkomponenten von einem System aus zu konfigurieren, kontrollieren und überwachen. Mit Ihrem Router haben Sie ein solches SNMP-Werkzeug erhalten, den ➤➤ **DIME Browser**. Da SNMP ein genormtes Protokoll ist, können Sie aber auch beliebige andere SNMP-Manager wie z. B. HP-Openview verwenden.

SNMP-Shell Eingabe-Ebene für SNMP-Kommandos.

SOHO Small Offices and Home Offices

Kleine Büros und Heimarbeitsplätze.

STAC Datenkomprimierungsverfahren.

Subnetz Ein Netzwerkschema, das einzelne logische Netzwerke in kleinere physikalische Einheiten teilt.

Switch LAN-Switches sind Netzwerkkomponenten, die der Funktion von ➤➤ **Bridges** oder sogar von ➤➤ **Routern** ähnlich sind. Sie vermitteln Datenpakete zwischen Ein- und Ausgangsport. Im Gegensatz zu Bridges haben Switches allerdings mehrere Ein- und Ausgangsports. Dadurch erhöht sich die Bandbreite im Netz. Switches können auch eingesetzt werden, um zwischen verschieden schnellen Netzen (z. B. 100MBit- und 10MBit-Netzen) zu übersetzen.

synchron Übertragungsverfahren, bei dem Sender und Empfänger in genau gleichen Zeittakten arbeiten – im Gegensatz zu ➤➤ **asynchron**. Leerzeichen werden durch eine Pausencodierung überbrückt.

TAPI Telephony Applications Programming Interface

Standardisierte Software-Schnittstelle von Mircrosoft, die von vielen Telefonie-Programmen verwendet wird. Telefonie-Programme ermöglichen datenbankgestütztes Telefonieren am Rechner. Ein Beispiel ist die Wahlhilfe von Windows oder das Programm orgAnice, das sich auf der BinTec Companion CD befindet. TAPI-Dienste werden nur von Routern mit integrierter ➤➤ **PABX** unterstützt.

Über die Remote TAPI von BinTec können alle Teilnehmer eines Netzes TAPI-Dienste nutzen.

TCP Transmission Control Protocol

Gehört zur Protokollfamilie ➤➤ **TCP/IP** zum Verbinden von Wide Area Networks (➤➤ **WANs**).

TCP/IP Transmission Control Protocol/Internet Protocol

Protokollfamilie zum Verbinden von Wide Area Networks (➤➤ **WANs**). Die beiden Bestandteile dieser Protokollfamilie sind ➤➤ **IP** (Schicht 3 des OSI-Modells) und ➤➤ **TCP** (Schicht 4 des OSI-Modells).

Telematik Telematik bezeichnet eine Kombination aus Telekommunikation und Computertechnik und beschreibt die Datenkommunikation zwischen Systemen und Geräten.

Telnet Protokoll aus der ➤➤ **TCP/IP-Protokollfamilie**. Telnet ermöglicht die Kommunikation mit einem anderen entfernten Gerät im Netzwerk.

TFTP Trivial File Transfer Protocol

Protokoll zum Übertragen von Daten.

Die TFTP-Server-Software ist Bestandteil der ➤➤ **DIME Tools**. Sie wird zum Übertragen von Konfigurationsdateien und Software vom und zum Router verwendet.

TK-Anlage Telekommunikationsanlage

Eine ISDN TK-Anlage ermöglicht das Einrichten einer internen Telefoninfrastruktur. An eine TK-Anlage lassen sich neben digitalen auch analoge Endgeräte (z. B. Faxgerät, Modem) anschließen. Im internen Netz kann man kostenlos telefonieren oder weiterverbinden. Die einzelnen Endgeräte erhalten unterschiedliche Rufnummern.

UDP User Datagram Protocol

Ein Transportprotokoll ähnlich ➤➤ **TCP**. UDP bietet keine Kontroll-/Quittierungsmechanismen, ist dafür aber schneller als TCP. UDP ist im Gegensatz zu TCP verbindungslos.

V.42bis Datenkomprimierungsverfahren.

VJHC Van Jacobsen Header-Komprimierung

Verfahren zur Datenkompression. IP-Header-Komprimierung.

Wählverbindung Eine Verbindung wird bei Bedarf durch Wählen einer Rufnummer aufgebaut, im Gegensatz zu einer ➤➤ **Festverbindung**.

WAN Wide Area Network

Weitverkehrsdatennetz, Verbindungen z. B. über ISDN, X.25.

WAN-Interface WAN-Schnittstelle.

WAN-Schnittstellen verbinden das lokale Netzwerk mit dem Weitverkehrsnetzwerk (➤➤ **WAN**). Üblicherweise dienen dazu analoge oder digitale Telefonleitungen (➤➤ **Wähl**- oder ➤➤ **Festverbindungen**).

WAN-Partner Gegenstelle, die über das ➤➤ **WAN**, z. B. ISDN, erreicht wird.

X.21 Die Empfehlungen aus X.21 definieren die physikalische Schnittstelle zwischen zwei Netzwerkkomponenten in einem Paketvermittlungsnetz (z. B. Datex-P).

X.25 Protokoll, das die Schnittstelle von Netzwerkkomponenten zu einem Paketvermittlungsnetz definiert.