X4100/200/300

Benutzerhandbuch

Installation und Konfiguration

Version 1.2
Dokument #70000M
April 2003

Ziel und Zweck

Dieses Handbuch beschreibt die Installation und Erstkonfiguration von **X4100/200/300** mit Software-Release 6.1. Für neueste Informationen und Hinweise zum aktuellen Software-Release sollten Sie in jedem Fall zusätzlich unsere **Release Notes** lesen – insbesondere, wenn Sie ein Software-Update zu einem höheren Release-Stand durchführen. Die aktuellsten **Release Notes** sind immer zu finden unter www.bintec.de.

Haftung

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

Die Informationen in diesem Handbuch können ohne Ankündigung geändert werden. Zusätzliche Informationen, sowie Änderungen und **Release Notes** für **X4100/200/300** finden Sie unter www.bintec.de.

Als Multiprotokollrouter baut **X4100/200/300** in Abhängigkeit von der Systemkonfiguration WAN-Verbindungen auf. Um ungewollte Gebühren zu vermeiden, sollten Sie das Produkt unbedingt überwachen. BinTec Access Networks GmbH übernimmt keine Verantwortung für Datenverlust, ungewollte Verbindungskosten und Schäden, die durch den unbeaufsichtigten Betrieb des Produkts entstanden sind.

Marken

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

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

Copyright

Richtlinien und Normen

X4100/200/300 entspricht folgenden Richtlinien und Normen:

- R&TTE-Richtlinie 1999/5/EC
- CE-Zeichen für alle EU-Länder und Schweiz

Weitere Informationen finden Sie in den "Declarations of Conformity" unter www.bintec.de.

Wie Sie BinTec erreichen

BinTec Access Networks GmbH
Südwestpark 94
D-90449 Nürnberg
Germany

Telephone: +49 911 96 73 0

Fax: +49 911 688 07 25

Internet: www.bintec.de

Kontaktinformationen für BinTec France finden Sie unter: www.bintec.fr.

Inhaltsverzeichnis 5

1 Willkommen

Mit **X4100/200/300** haben Sie sich zum Kauf eines erweiterbaren Multiprotokoll-Routers der Workgroup-Access-Reihe von BinTec Access Networks GmbH entschieden – eine leistungsfähige und zukunftssichere Router-Lösung für den Einsatz in kleinen und mittleren Betrieben.

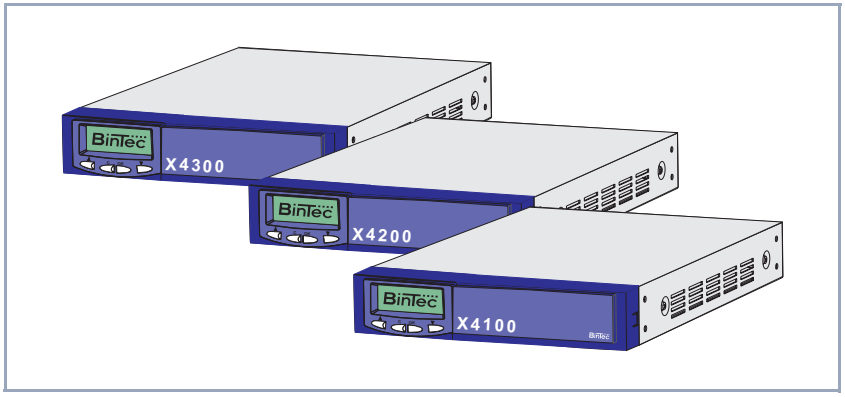


Bild 1-1: **X4100/200/300** - der Workgroup-Access-Router für heute und morgen

X4100/200/300 realisiert mit nur einem Grundgerät vielfältige Anwendungsmöglichkeiten:

- Router für Festverbindungen mit ISDN-Backup
- Router für analoge und digitale Verbindungen
- VPN-Lösung mit Datenverschlüsselung und ISDN-Backup
- Remote-Access-Server für bis zu 62 Verbindungen
- "Quality of Service" ermöglicht die effektive Nutzung vorhandener Bandbreite
- "xDSL" unterstützt Breitbandtechnologien wie ADSL, SDSL, Kabelmodems usw.
- Sichere Unternehmenskommunikation durch starke Datenverschlüsselung mit IPSec (optional)
- Zentrales Fax-Gateway für bis zu 30 Verbindungen in Vorbereitung

1.1 X4100/200/300 – Workgroup-Access-Router für Heute und Morgen

Die Erweiterbarkeit von **X4100/200/300** macht den Multiprotokollrouter zu einer zukunftssicheren und flexibel einsetzbaren Investition. Ausgestattet mit einer RISC-CPU ist **X4100/200/300** extrem leistungsfähig und auch zukünftigen Anforderungen gewachsen.

Grundgerät

Die Grundgeräte können mittels Winkel in einen 19-Zoll-Schrank eingebaut werden. Zur Grundausstattung der Grundgeräte gehört eine 10/100 BT-Ethernet-Schnittstelle, eine ISDN-BRI-Schnittstelle und eine serielle Konsolenschnittstelle.

Das Grundgerät von **X4100** verfügt zusätzlich zur Grundausstattung über eine 10 BT-Ethernet-Schnittstelle für xDSL.

Das Grundgerät von **X4200** verfügt zusätzlich zur Grundausstattung über eine 10 BT-Ethernet-Schnittstelle für xDSL und eine serielle X.21/V.35-Schnittstelle für Festverbindungen.

Das Grundgerät von **X4300** verfügt zusätzlich zur Grundausstattung über zwei serielle X.21/V.35-Schnittstellen für Festverbindungen.

Erweiterungskarten

Ein Steckplatz für eine von außen steckbare Erweiterungskarte ermöglicht **X4100/200/300**, mit Ihren Anforderungen zu wachsen und dasselbe Grundgerät für verschiedene Applikationen einzusetzen. Hohe Flexibilität ist gewährleistet.

Ressourcenkarten

Alle Erweiterungskarten sind zusätzlich mit leistungsfähigen Ressourcenkarten auszustatten. So kann eine außerordentlich hohe Leistungsfähigkeit und Port- bzw. Modemdichte erreicht werden. Die Ressourcenkarten sind bestückt mit Digitalmodems für analoge Verbindungen oder mit Verschlüsselungs- und Kompressionsmodulen (HiFn). HiFn verschlüsselt die Daten für die sichere Datenübertragung.

Multiprotokollrouter

Der flexible Multiprotokollrouter kann für den WAN-Access, aber auch als Remote-Access-Server, LAN-Router, Remote-CAPI-Server oder Fax-Gateway (in Vorbereitung) eingesetzt werden. **X4100/200/300** unterstützt die Protokolle der

Protokollfamilie TCP/IP und X.25 (optional) und beherrscht das Bridging von weiteren Protokollen nach dem Spanning-Tree-Verfahren.

Remote-CAPI Mit Hilfe von BinTecs Remote-CAPI-Schnittstelle können Applikationen, die auf der weitverbreiteten CAPI-Schnittstelle aufsetzen, netzwerkweit eingesetzt werden. Die vorhandenen ISDN-Anschlüsse können so effektiver genutzt werden.

Sicherheit BinTecs erprobtes Sicherheitspaket SAFERNET™ ist im Lieferumfang enthalten. Es beinhaltet Security-Technologien wie z. B. Filter, Network Address Translation (NAT) und Zugangspaßwörter. Die Sicherheitsfunktionen schützen **X4100/200/300** und das daran angeschlossene Netzwerk vor unerlaubtem Zugriff. Optional ist IPSec erhältlich. Mit **X4100/200/300** können Sie VPNs (PPTP) realisieren.

Quality of Service Immer mehr Anwendungen benötigen immer größere Bandbreiten. Nicht immer stehen diese zur Verfügung. "Quality of Service" (QoS) ermöglicht es, die vorhandene Bandbreite zu nutzen und die verfügbaren Ressourcen effektiv und intelligent zu verteilen. Bestimmte Anwendungen können bevorzugt behandelt und Bandbreite für diese reserviert werden. Vor allem für zeitkritische Anwendungen wie VoIP, SAP usw. ist dies von enormem Vorteil.

xDSL/Kabelmodem Die Grundgeräte **X4100** und **X4200** verfügen über zwei Ethernet-Schnittstellen. Sie sind daher ideal für den Betrieb an verschiedenen DSL-Modems (ADSL, SDSL, usw.) oder an einem Kabelmodem.

IPSec **X4100/200/300** kann optional um eine vollständige IPSec-Software erweitert werden, die Interoperabilität mit IPSec-Software von vielen anderen Herstellern gewährleistet. Diese Software unterstützt Leistungsmerkmale wie "Internet Key Exchange", "pre-shared keys", "Public Key Infrastructure", X.509v3-Zertifikate, Tunnel- und Transportmodus sowie die Verschlüsselungsverfahren DES, Triple DES, CAST und Blowfish mit Schlüssellängen bis zu 168 Bit.

Zukunft Neue Technologien und Entwicklungen sind der BinTec Access Networks GmbH ein Anliegen. Die flexible Plattform **X4100/200/300** mit einem Erweiterungssteckplatz und der leistungsfähige Prozessor ermöglichen den kurzfristigen Einsatz von neuen WAN-/LAN-Technologien und Features. Somit ist **X4100/200/300** zukunftssicheres und migrationsfähiges Gerät.

Aktuelle Software wird von BinTec kostenlos über das World Wide Web zum Download zur Verfügung gestellt.

Detailliertere Informationen zu den einzelnen Themen finden Sie an entsprechenden Stellen dieses Handbuchs und in der weiterführenden Dokumentation (zu finden auf der BinTec Companion CD).

1.2 Lieferumfang

Dieses Kapitel beschreibt den Lieferumfang der Grundgeräte und der Erweiterungskarten.

1.2.1 Grundgerät

Das **X4100/200/300**-Grundgerät ist ein 19-Zoll-Einbaugerät. Zusammen mit dem **X4100/200/300**-Grundgerät werden folgende Teile ausgeliefert:

- Kabelsätze
  - Serielles Anschlußkabel für den Konsolenport
  - Kaltgeräte-Netzkabel
  - ISDN-Kabel
- BinTec Companion CD
- Dokumentation
  - **Benutzerhandbuch**
  - **Release Notes**, falls erforderlich
- Satz 19-Zoll-Befestigungsmaterial

1.2.2 Erweiterungskarten

Folgende Erweiterungskarten für **X4100/200/300** können erworben werden:

- X4E-1/2PRI: WAN-Schnittstellenkarte für ISDN-PRI und/oder G.703
  - im Auslieferungszustand ausgestattet mit Hardware-Unterstützung (HiFn) für Verschlüsselung und Kompression
  - optional auszustatten mit bis zu zwei Ressourcenkarten (XT-S, XT-M, XT-2M, XT-L) mit maximal 30 Digitalmodems.
- X4E-2/3BRI: WAN-Schnittstellenkarte für ISDN-BRI, optional auszustatten mit
  - einer Ressourcenkarte mit Digitalmodems (XT-S, XT-M) und/oder

  - einer Ressourcenkarte zur Verschlüsselung und Kompression (XT-ENC)

- X4E-2FE: LAN-Schnittstellenkarte für 10/100 MBit/s, optional auszustatten mit
  - einer Ressourcenkarte zur Verschlüsselung und Kompression (XT-ENC)

1.3 BinTec Companion CD

Auf Ihrer BinTec Companion CD finden Sie alle Programme, die Sie zur Installation, Konfiguration und Wartung von **X4100/200/300** brauchen.

BRICKware

BRICKware for Windows enthält die Windows-Hilfsprogramme:

- Die **DIME Tools** dienen der Überwachung und Administration von **X4100/200/300**.
- Über das Terminal-Programm **Gerät an COM1** bzw. **Gerät an COM2** erhalten Sie Zugang zu **X4100/200/300** über die serielle Schnittstelle.
- Der **Configuration Manager** erlaubt es Ihnen, alle BinTec-Router im Netz über eine graphische Oberfläche zu konfigurieren und administrieren. Hier können Sie SNMP-Tabellen und -Variablen einsehen und bearbeiten.
- Remote-CAPI-Client:
  Mit dem Remote-CAPI-Client können Sie Kommunikationsanwendungen nutzen, die auf die genormte CAPI-Schnittstelle aufsetzen.
- Token Authentication Firewall (TAF) Programm (optional):
  Dieses Softwarepaket benötigen Sie, wenn Sie das Sicherheitssystem von Security Dynamics verwenden.
- Mit dem Activity Monitor können Sie die Auslastung von **X4100/200/300** mit einem Blick überwachen.

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

Was sonst?

Auf der Companion CD finden Sie eine Reihe weiterer nützlicher Verzeichnisse, z. B. mit folgendem Inhalt:

- Die Dokumentation in elektronischer Form (siehe Kapitel 1.4, Seite 20)
- Eine Kopie der Router-Software
- UNIX-Tools (Administration)
- Adobe Acrobat Reader

1.4 Dokumentation bei BinTec

Derzeit ist folgende Dokumentation verfügbar:

- **Benutzerhandbuch** (deutsch)
  Dieses Handbuch.
- 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.
  - **MIB Reference**
    HTML-Dokument mit Kurzbeschreibungen zu allen SNMP-Tabellen und Variablen von **X4100/200/300**.
- **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 Notes Logic** finden Sie eine Anleitung zum Upgrade von Bootmonitor und/oder Firmware-Logic.
- **Release Notes** für den Routerbetrieb in UK (englisch, PDF)
  Hinweise zum Betrieb von BinTec-Routern in Großbritannien.

Die Dokumentation haben Sie zusammen mit **X4100/200/300** erhalten. In gedruckter Form liegt Ihnen das Benutzerhandbuch vor. Auf Ihrer BinTec Companion CD finden Sie außerdem die gesamte Dokumentation in elektronischer Form (PDF, HTML). Zusätzlich zur Companion CD stehen alle Dokumente jeweils in der aktuellen Version auf unserem WWW-Server unter www.bintec.de kostenlos zum Download bereit.

1.5 Systemvoraussetzungen

X4100/200/300 können Sie von allen herkömmlichen Plattformen aus konfigurieren. Als Standalone-Gerät ist **X4100/200/300** nicht vom angeschlossenen Rechner oder dessen Betriebssystem abhängig. Die Kommunikation zum Rechner erfolgt über ISDN-Login, eine LAN-Schnittstelle (10/100 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.

1.6 Zu diesem Handbuch

Dieses Kapitel beschreibt kurz den Inhalt der einzelnen Kapitel und die Verwendung der Symbole und Auszeichnungselemente.

1.6.1 Inhalt

Das Handbuch ist folgendermaßen aufgebaut:

Kapitel	Inhalt
1: "Willkommen"	Allgemeine Einführung, Lieferumfang, Informationen zu diesem Handbuch.
2: "Allgemeine Sicherheitshinweise"	Allgemeine Sicherheitshinweise in deutsch.
3: "Beschreibung und Installation der Hardware"	Beschreibung der Hardware (Grundgerät, Erweiterungskarten, MMI, LEDs, Anschlüsse). Anweisungen, wie Sie das 19-Zoll-Einbaugerät im Rack einbauen, wie Sie das Display umstekken können, wie Sie eine Erweiterungskarte ein- bzw. ausbauen und wie Sie das Gerät anschließen. Beschreibung der Boot-Sequenz.
4: "Voraussetzungen für die Konfiguration"	Beschreibung der Zugangs- und Konfigurationsmöglichkeiten. Grundlagen zum Umgang mit dem Setup Tool. Vorgehensweise für eine Initialkonfiguration.
5: "Man Machine Interface (MMI) – Display mit Benutzerführung"	Wie Sie das MMI mit Display und Eingabetasten nutzen können.
6: "Basiskonfiguration des Grundgeräts mit dem Setup Tool"	Wie Sie **X4100/200/300** mit dem Setup Tool in Betrieb nehmen und eine Grundkonfiguration einrichten (einschließlich der Konfiguration der WAN-Schnittstellen).

Kapitel	Inhalt
7: "Weiterführende Konfiguration des Grundgeräts mit dem Setup Tool"	Wie Sie weitere Konfigurationseinstellungen mit dem Setup Tool vornehmen.
8: "Konfiguration der Erweiterungs- und Ressourcenkarten mit dem Setup Tool"	Wie Sie eine Erweiterungskarte und gegebenenfalls Ressourcenkarte(n) konfigurieren.
9: "Konfiguration von Sicherheitsfunktionen"	Wie Sie Sicherheitsmechanismen von SAFERNET einrichten, z. B. NAT (Network Address Translation) oder Filter.
10: "Konfigurationsmanagement"	Wie Sie Konfigurationsdateien verwalten und Software-Updates durchführen.
11: "Troubleshooting"	Wichtige Hinweise zur Fehlerbehebung.
12: "Technische Daten"	Die Technischen Daten von **X4100/200/300**.
13: "Wichtige Kommandos"	Eine Kurzübersicht zu den wichtigsten Befehlen und Kommandos der SNMP-Shell und der BRICKtools für Unix.
14: "Allgemeine Sicherheitshinweise in 15 Landessprachen"	Allgemeine Sicherheitshinweise in 15 Landessprachen.

Tabelle 1-1: Kapitelübersicht

1.6.2 Verwendung

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

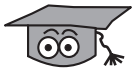
Symbol	Verwendung
	Kennzeichnet Stellen, an denen Tips gegeben werden.
	Kennzeichnet Stellen, an denen Hinweise zur Fehlerbehebung gegeben werden.
	Kennzeichnet allgemeine wichtige Hinweise.
	Kennzeichnet Stellen, an denen zusätzliches Hintergrundwissen erläutert wird.
	Kennzeichnet Warnhinweise. Einteilung 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 kann)

Tabelle 1-2: Symbolübersicht

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*** **Datei ➧ Öffnen**	Kennzeichnung von Menüs und Untermenüs im Setup Tool. Kennzeichnung von Menüs und Untermenüs in der Windows-Oberfläche.
`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.
`<IP address>`	Kennzeichnung von Eingaben, bei der Sie den in Klammern gesetzten Ausdruck durch Ihren Wert ersetzen. Die spitzen Klammern fallen bei der Eingabe weg.
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 im Setup Tool oder bei MIB-Variablen eingetragen bzw. eingestellt werden können.
Online: blau	Kennzeichnung von Links.

Tabelle 1-3: Auszeichnungselemente

1.7 Feedback

Als Dokumentationsteam bei BinTec Access Networks GmbH schreiben wir Handbücher und andere Dokumentationen für Sie. Wir wollen zu einem hochwertigen Produkt wie **X4100/200/300** eine ebenso hochwertige Dokumentation liefern, um Ihren Ansprüchen gerecht zu werden. Ob uns das mit diesem Handbuch gelungen ist, können Sie als Nutzer(in) von BinTec-Produkten am besten beurteilen.

Teilen Sie uns deswegen doch einfach mit, was Ihnen im Handbuch fehlt, was Sie stört, was wir besser machen sollten, was Ihnen gefällt, was Sie besonders gelungen finden, etc. Ihre konstruktive Kritik ist uns jederzeit willkommen und wird uns helfen, die zu BinTec-Produkten gehörigen Dokumentationen Ihren Wünschen und Bedürfnissen entsprechend zu gestalten!

Fragebogen

Für Ihre Anregungen haben wir einen Fragebogen auf der letzten Seite dieses Handbuchs vorbereitet. Schicken Sie bitte den ausgefüllten Fragebogen

- per Fax an: 0911 - 688075
- per Post an:
  BinTec Access Networks GmbH
  Stichwort: Doku-Feedback
  Südwestpark 94
  90449 Nürnberg
- oder schreiben Sie uns einfach eine Email an:
  doku_feedback@bintec.de

Wir freuen uns auf Ihr Feedback und bedanken uns für Ihre Unterstützung!

2 Allgemeine Sicherheitshinweise

Allgemeine Sicherheitshinweise in deutsch

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

Transport und Lagerung

- Transportieren und lagern Sie **X4100/200/300** nur in der Originalverpakkung 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 **X4100/200/300** die Hinweise für die Umgebungsbedingungen (vgl. Technische Daten). Verwenden Sie eine feste und ebene Unterlage.
- Elektrostatische Aufladungen können zu Geräteschäden führen. Tragen Sie daher eine geerdete Manschette um das Handgelenk oder berühren Sie eine geerdete Fläche, bevor Sie Buchsen oder Erweiterungskarten von **X4100/200/300** berühren. Berühren Sie die Erweiterungskarten grundsätzlich nur an den Rändern und fassen Sie nicht auf Bauteile oder Leiterbahnen.
- Halten Sie den nicht benutzten Erweiterungssteckplatz mit der Blindabdekkung verschlossen, damit keine Gegenstände ins Innere des Gerätes gelangen können. Befinden sich während des Betriebs Fremdgegenstände im Gerät, besteht Stromschlag- und Kurzschlußgefahr.
- Achten Sie darauf, daß keine spitzen Gegenstände das Fenster des Displaymoduls beschädigen. Schützen Sie das Displaymodul vor Stoß und Fall und schließen Sie es nur an die dafür vorgesehene RJ11-Buchse von **X4100/200/300** an, um Schäden an **X4100/200/300** und dem Displaymodul zu vermeiden.
- Achten Sie bei der Verkabelung darauf, daß die Lüftungsschlitze des Geräts nicht verdeckt werden und die Lüftung nicht behindert wird. Durch Beeinträchtigung der Lüftung von **X4100/200/300** kann es zu Schäden am Gerät kommen. Durch mangelnde Lüftung entstandene Schäden führen zum Garantieverlust.

- Öffnen Sie nicht das Grundgerät und nehmen Sie keinerlei Manipulationen am Netzteil vor, da sonst Lebensgefahr durch einen Stromschlag besteht. Entfernen Sie keine Befestigungsschrauben des Grundgerätes.
- 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 Gerät temperaturangeglichen und absolut trokken ist, bevor Sie es in Betrieb nehmen. Beachten Sie die Umweltbedingungen in den Technischen Daten.
- Prüfen Sie, ob die örtliche Netzspannung mit den Nennspannungen des Netzteils übereinstimmt. Das Gerät darf unter folgenden Bedingungen betrieben werden:
  - 100 - 240 VAC
  - 50/60 Hz
- Stellen Sie sicher, daß die Schutzkontakt-Steckdose der Installation frei zugänglich ist. Zur vollständigen Netztrennung muß der Netzstecker gezogen werden.
- Beachten Sie beim Verkabeln die Reihenfolge, wie im Handbuch beschrieben. Verwenden Sie nur Kabel, die den Spezifikationen in diesem Handbuch genügen oder original mitgeliefert wurden. Falls Sie andere Kabel verwenden, übernimmt BinTec Access Networks GmbH für auftretende Schäden oder Beeinträchtigung der Funktionalität keine Haftung. Die Gerätegarantie erlischt in diesen Fällen.
- Beachten Sie beim Anschluß des Geräts die Hinweise im Handbuch.
- 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 oder berühren Sie diese.

Bestimmungsgemäße Verwendung, Betrieb

- **X4100/200/300** ist für den Einsatz in einer Büroumgebung bestimmt. Als Multiprotokoll-Router baut **X4100/200/300** in Abhängigkeit von der Systemkonfiguration WAN-Verbindungen auf. Um ungewollte Gebühren zu vermeiden, sollten Sie das Produkt unbedingt überwachen.

- **X4100/200/300** 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 komplett montiertem Blechgehäuse gewährleistet (Kühlung, Brandschutz, Funkentstörung).
- Die Umgebungstemperatur darf 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.
- **X4100/200/300** enthält keine Bauteile, die vom Benutzer getauscht werden dürfen oder Schalter/Jumper, die der Benutzer einstellen muß.
- Unterbrechen Sie in Notfällen (z. B. beschädigtes Gehäuse oder Bedienelement, Eindringen von Flüssigkeit oder Fremdkörpern) sofort die Stromversorgung und verständigen Sie den Service.

Reinigung und Reparatur

- Das Gerät darf nur von einer BinTec-autorisierten Servicestelle geöffnet werden. Vor Öffnen des Geräts unbedingt den Netzstecker ziehen. Durch unbefugtes Öffnen und unsachgemäße Reparaturen können erhebliche Gefahren für den Benutzer entstehen (z. B. Stromschlag). Lassen Sie Reparaturen am Gerät nur von einer BinTec-autorisierten Servicestelle durchführen. Wo sich die Servicestelle befindet, erfahren Sie von Ihrem Händler. In allen anderen Fällen erlöschen jegliche Garantieansprüche.
- 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 Beschreibung und Installation der Hardware

Dieses Kapitel beschreibt folgendes:

- Grundgerät, Kapitel 3.1, Seite 32
- Einbau in den 19-Zoll-Schrank, Kapitel 3.2, Seite 36
- Erweiterungs- und Ressourcenkarten, Kapitel 3.3, Seite 39
  - Schnittstellen und LEDs der Erweiterungskarten, Kapitel 3.3.1, Seite 39
  - Einbau und Austausch einer Erweiterungskarte, Kapitel 3.3.2, Seite 42
- Aufstellen und Anschließen von **X4100/200/300**, Kapitel 3.4, Seite 46
- Statusmeldungen über Leuchtdioden (LEDs), Kapitel 3.5, Seite 49
- Boot-Sequenz, Kapitel 3.6, Seite 52

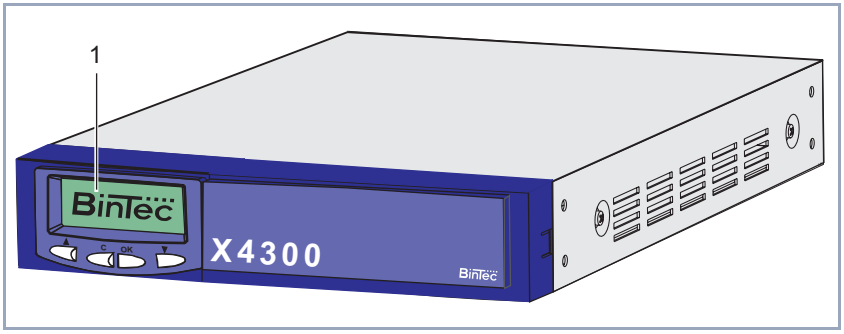
3.1 Grundgerät

Das **X4100/200/300-**Grundgerät ist mittels Winkel in einen 19-Zoll-Schrank einzubauen (siehe Kapitel 3.2, Seite 36).

Das **X4100/200/300-**Grundgerät enthält im Auslieferungszustand keine Erweiterungskarte. Der für die Erweiterungskarte vorgesehene Erweiterungssteckplatz auf der Geräterückseite ist mit einer Blindabdeckung verschlossen. Diese wird beim späteren Einbau einer Erweiterungskarte abgeschraubt und beim Stecken einer Erweiterungskarte automatisch durch die Backplane der eingebauten Erweiterungskarte ersetzt.

3.1.1 Vorderseite des Grundgerätes

Die Vorderseiten der Grundgeräte von **X4100**, **X4200** und **X4300** sind – bis auf die Gerätebezeichnung - identisch:



1	Display mit Eingabetasten (MMI)		

Bild 3-1: Vorderansicht Grundgerät

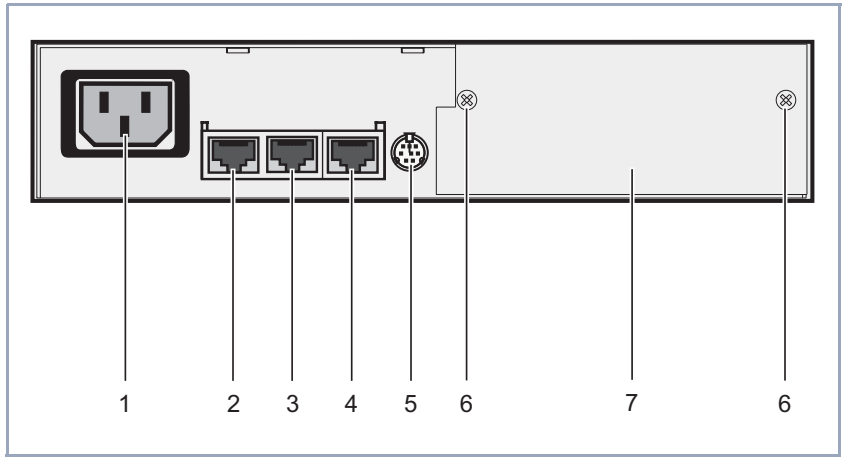
Display und Eingabetasten

BinTecs Man Machine Interface (MMI), eine komfortable Benutzerführung mit Display und Eingabetasten, führt Sie durch einige grundlegende Funktionen von **X4100/200/300**. Die genaue Funktionsbeschreibung des MMI finden Sie in Kapitel 5, Seite 83.

3.1.2 Rückseite der unterschiedlichen Grundgeräte

Die Anschlüsse von X4100

Rückansicht des Grundgerätes **X4100**:

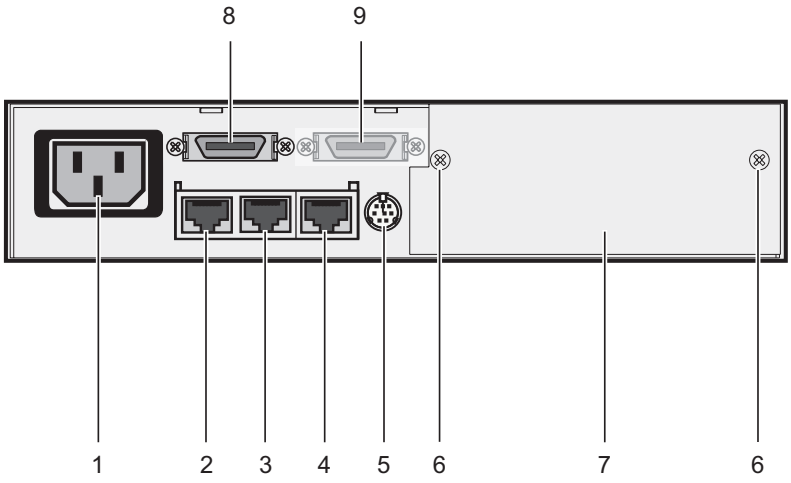


1	Kaltgerätebuchse des Netzteils	5	Mini-DIN-Buchse (Konsole)
2	ISDN-BRI-Schnittstelle	6	Befestigungsschrauben der Erweiterungskarte bzw. der Blindabdeckung
3	Ethernet/LAN-Schnittstelle 10/100 Base-T Fast Ethernet	7	Erweiterungskartensteckplatz (mit Blindabdeckung)
4	10 Base-T Ethernet für xDSL		

Bild 3-2: Rückansicht **X4100**

Die Anschlüsse von X4200

Rückansicht des Grundgerätes **X4200**:

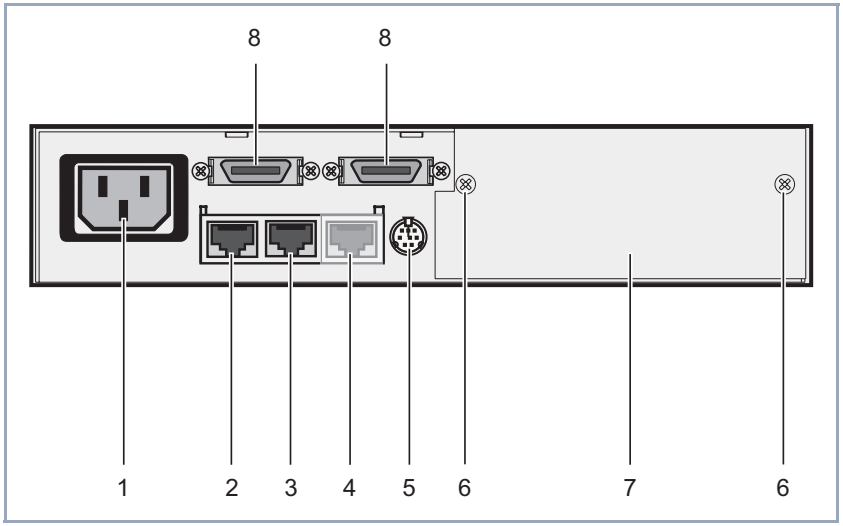


1	Kaltgerätebuchse des Netzteils	6	Befestigungsschrauben der Erweiterungskarte bzw. der Blindabdeckung
2	ISDN-BRI-Schnittstelle	7	Erweiterungskartensteckplatz (mit Blindabdeckung)
3	Ethernet/LAN-Schnittstelle 10/100 Base-T Fast Ethernet	8	X.21/V.35-Schnittstelle
4	10 Base-T Ethernet für xDSL	9	nicht belegt (X.21/V.35-Schnittstelle)
5	Mini-DIN-Buchse (Konsole)		

Bild 3-3: Rückansicht **X4200**

Die Anschlüsse von X4300

Rückansicht des Grundgerätes **X4300**:



1	Kaltgerätebuchse des Netzteils	5	Mini-DIN-Buchse (Konsole)
2	ISDN-BRI-Schnittstelle	6	Befestigungsschrauben der Erweiterungskarte bzw. der Blindabdeckung
3	Ethernet/LAN-Schnittstelle 10/100 Base-T Fast Ethernet	7	Erweiterungskartensteckplatz (mit Blindabdeckung)
4	nicht belegt (10 Base-T Ethernet für xDSL)	8	X.21/V.35-Schnittstellen

Bild 3-4: Rückansicht **X4300**

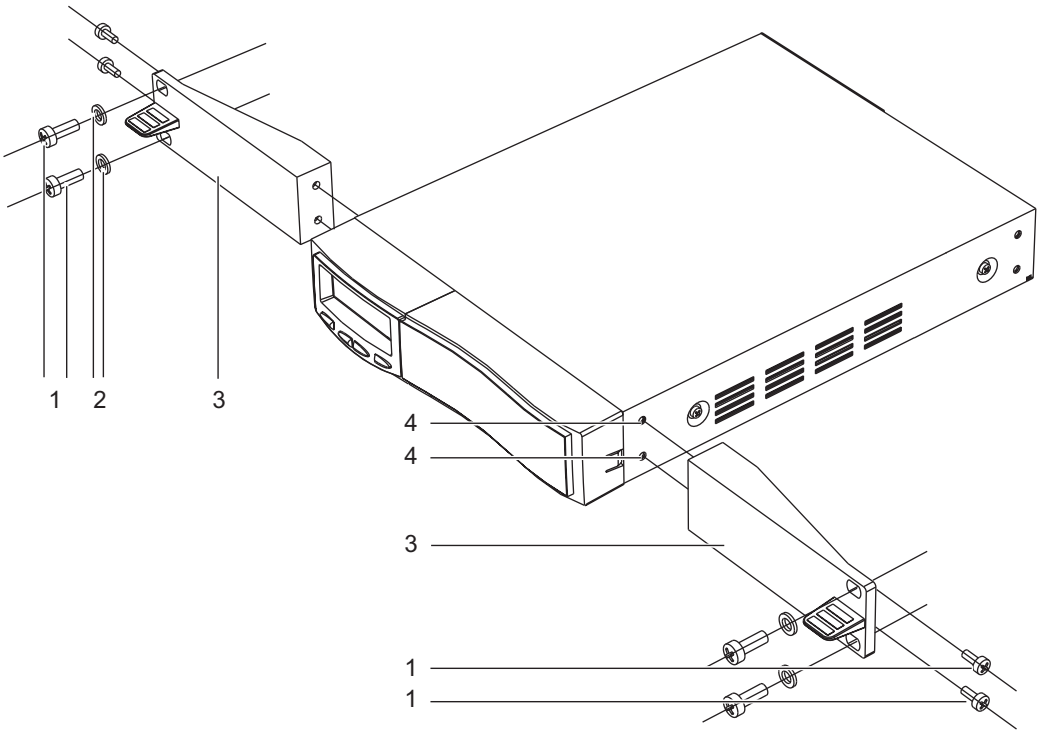
Anschließen

Zum Anschließen Ihres Grundgeräts gehen Sie zu Kapitel 3.4, Seite 46.

3.2 Einbau in den 19-Zoll-Schrank

Die Grundgeräte der **X4100/200/300** können in einen 19-Zoll-Schrank eingebaut werden.

Hier eine grafische Darstellung der Bau- und Befestigungsteile für den Einbau in einen 19-Zoll-Schrank:



1	Schrauben	3	Befestigungswinkel
2	Unterlegscheiben	4	Befestigungslöcher

Bild 3-5: Explosionszeichnung mit den wichtigsten Bau- und Befestigungsteilen für den Einbau der Grundgeräte in einen 19-Zoll-Schrank

Winkel befestigen So werden die Winkel am Grundgerät befestigt:

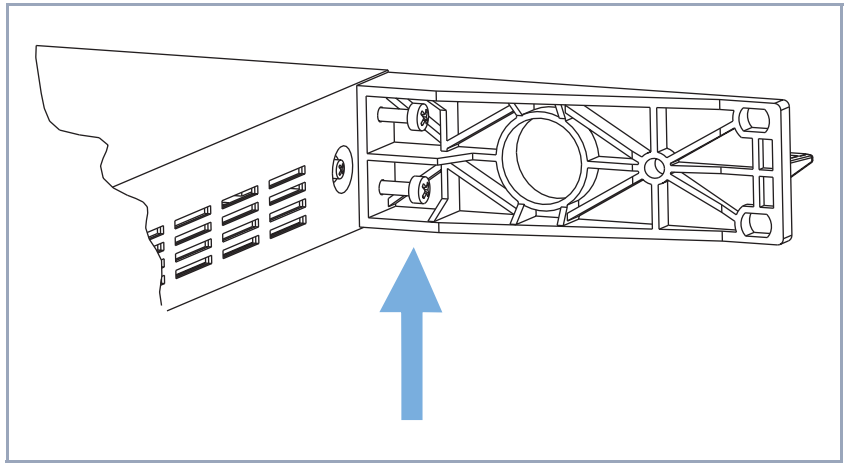


Bild 3-6: Winkel an Befestigungslöcher festschrauben

Gehen Sie folgendermaßen vor:

- Schrauben Sie die beiden mitgelieferten Befestigungswinkel (3, siehe Bild 3-5, Seite 36) mit den mitgelieferten Schrauben (1, siehe Bild 3-5, Seite 36) und Unterlegscheiben (2, siehe Bild 3-5, Seite 36) an die Befestigungslöcher (4, siehe Bild 3-5, Seite 36) von **X4100/200/300**, wie in Bild 3-6, Seite 37 dargestellt.
  Verwenden Sie unbedingt die mitgelieferten Schrauben. Andere Schrauben halten eventuell den mechanischen Belastungen nicht stand oder können das Gerät zerstören.
- Stecken Sie die benötigten Schnittstellenkabel jetzt in die dafür vorgesehenen Buchsen (siehe Kapitel 3.4, Seite 46), insbesondere wenn Ihr Schrank nicht von der Rückseite zugänglich ist.
- Schieben Sie diese vormontierte Einheit mit den beiden angeschraubten Winkeln in Ihren 19-Zoll-Schrank und verschrauben Sie die vormontierte Einheit mit den Längsprofilen des Schranks.
  Diese Schrauben sind nicht im Lieferumfang von **X4100/200/300** enthalten, sondern sind Bestandteil des Lieferumfangs Ihres 19-Zoll-Schrankes.

So sollte Ihr Grundgerät montiert aussehen:

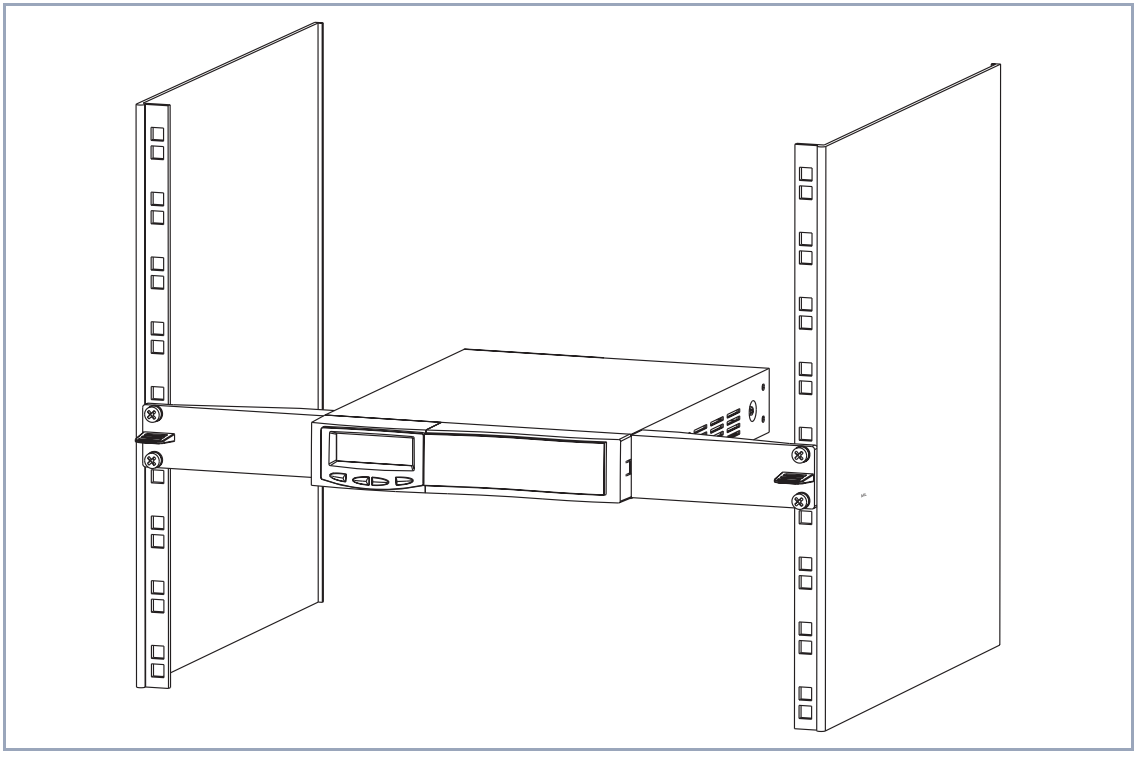


Bild 3-7: Grundgerät montiert im 19-Zoll-Schrank

Zum Anschließen Ihres 19-Zoll-Einbaugeräts gehen Sie zu Kapitel 3.4, Seite 46.

Ausbau aus einem 19-Zoll-Schrank

Zum Ausbau von **X4100/200/300** aus dem 19-Zoll-Schrank (z. B. für den Tausch oder Einbau einer Erweiterungskarte, Einbau einer Lüfterkassette, etc.) führen Sie bitte die oben beschriebenen Schritte in umgekehrter Reihenfolge durch.

3.3 Erweiterungs- und Ressourcenkarten

Mit einer **X4100/200/300-**Erweiterungskarte können Sie Ihr Grundgerät erweitern.

Folgende Erweiterungskarten werden von BinTec für die Integration in **X4100/200/300** angeboten:

- X4E-1/2PRI: WAN-Schnittstellenkarte für ISDN-PRI und/oder G.703
  - im Auslieferungszustand ausgestattet mit Hardware-Unterstützung für Verschlüsselung und Kompression
  - optional auszustatten mit bis zu zwei Ressourcenkarten (XT-S, XT-M, XT-2M, XT-L) mit Digitalmodems.
- X4E-2/3BRI: WAN-Schnittstellenkarte für ISDN-BRI, optional auszustatten mit
  - einer Ressourcenkarte mit Digitalmodems (XT-S, XT-M) und/oder
  - einer Ressourcenkarte zur Verschlüsselung und Kompression (XT-ENC)
- X4E-2FE: LAN-Schnittstellenkarte für 10/100 MBit/s, optional auszustatten mit
  - einer Ressourcenkarte zur Verschlüsselung und Kompression (XT-ENC)

Zur Konfiguration der Erweiterungs- und Ressourcenkarten beachten Sie bitte Kapitel 8, Seite 287. Die technischen Daten (einschließlich Pinbelegung der Schnittstellen) finden Sie in Kapitel 12.3, Seite 409.

3.3.1 Schnittstellen und LEDs der Erweiterungskarten

Im folgenden werden die Rückansichten der Erweiterungskarten mit den jeweils verfügbaren Schnittstellen und LEDs dargestellt.

Die Bedeutung der LEDs finden Sie in Kapitel 3.5.2, Seite 49 erklärt.

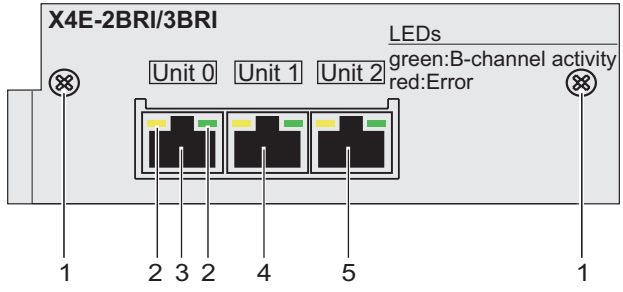
BRI-Erweiterungskarte X4E-2/3BRI

Achtung!

Der Einbau von Ressourcenkarten in eine Erweiterungskarte führt zu verstärkter Wärmeentwicklung. Um die Schädigung von Bauteilen zu vermeiden, ist der Einsatz einer Lüfterkassette zwingend erforderlich!

➤ Setzen Sie bei Verwendung einer Erweiterungskarte mit Ressourcenkarte(n) im **X4100/200/300**-Einbaugerät die Lüfterkassette ein.

Sie können die Lüfterkassette von Ihrem Lieferanten käuflich erwerben.



1	Befestigungsschrauben	2	LEDs
3	ISDN-BRI-Port, Unit 0	4	ISDN-BRI-Port, Unit 1
5	ISDN-BRI-Port, Unit 2		

Bild 3-8: Rückansicht einer BRI-Erweiterungskarte

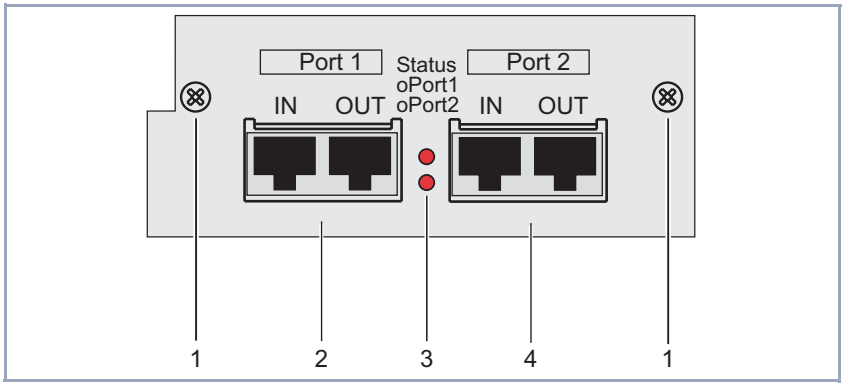
PRI/G.703-Erweiterungskarte X4E-1/2PRI

Achtung!

Der Einbau der PRI/G.703-Erweiterungskarte führt zu verstärkter Wärmeentwicklung. Um die Schädigung von Bauteilen zu vermeiden, ist der Einsatz einer Lüfterkassette zwingend erforderlich!

➤ Setzen Sie bei Verwendung der PRI/G.703-Erweiterungskarte im **X4100/200/300**-Einbaugerät die Lüfterkassette ein.

Sie können die Lüfterkassette von Ihrem Lieferanten käuflich erwerben.



1	Befestigungsschrauben	2	ISDN-PRI/G.703-Port mit IN- und OUT-Buchse, Port 1
3	LEDs	4	ISDN-PRI/G.703-Port mit IN- und OUT-Buchse, Port 2

Bild 3-9: Rückansicht einer PRI/G.703-Erweiterungskarte

Bei der PRI/G.703-Erweiterungskarte stehen pro Schnittstelle zwei RJ45-Buchsen zur Verfügung – IN und OUT.

Zum Anschließen der Erweiterungskarte verbinden Sie das Anschlußkabel mit der IN-Buchse. Über die OUT-Buchse können Sie optional einen Backup-Router anschließen, der beim Abschalten oder Ausfallen des ersten Routers dessen Funktion übernehmen kann.

Ferner kann durch Anbringen eines Loopback-Steckers auf der OUT-Buchse verhindert werden, daß die Vermittlungsstelle des Providers die Leitung bei Ausfall der Erweiterungskarte abschaltet.

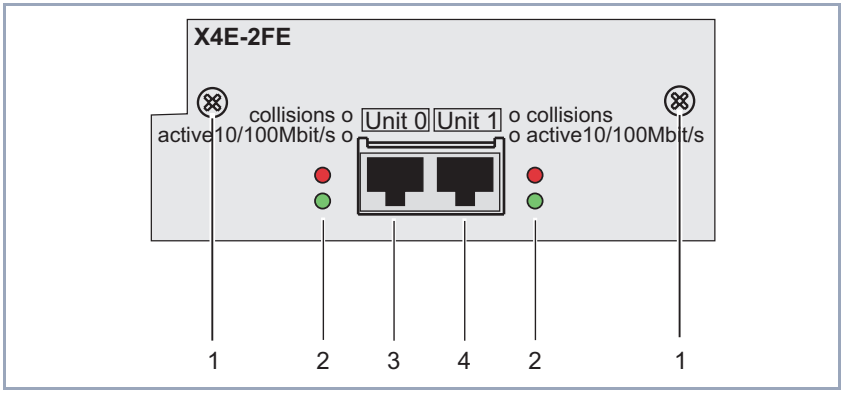
LAN-Erweiterungskarte X4E-2FE

Achtung!

Der Einbau von Ressourcenkarten in eine Erweiterungskarte führt zu verstärkter Wärmeentwicklung. Um die Schädigung von Bauteilen zu vermeiden, ist der Einsatz einer Lüfterkassette zwingend erforderlich!

➤ Setzen Sie bei Verwendung einer Erweiterungskarte mit Ressourcenkarte(n) im **X4100/200/300**-Einbaugerät die Lüfterkassette ein.

Sie können die Lüfterkassette von Ihrem Lieferanten käuflich erwerben.



1	Befestigungsschrauben	2	LEDs
3	Fast-Ethernet-Port, Unit 0	4	Fast-Ethernet-Port, Unit 1

Bild 3-10: Rückansicht einer LAN-Erweiterungskarte

3.3.2 Einbau und Austausch der Erweiterungskarte

Dieses Kapitel erläutert, wie Sie das **X4100/200/300-**Grundgerät mit einer Erweiterungskarte bestücken oder diese gegen eine der anderen **X4100/200/300**-

Erweiterungskarten austauschen können. Beachten Sie bitte auch die im Lieferumfang der Erweiterungs- und Ressourcenkarten enthaltene Einbauanleitung!

Achtung!

Der Einbau oder Austausch einer Erweiterungskarte darf nicht im laufenden Betrieb durchgeführt werden. **X4100/200/300** muß auf jeden Fall von der Stromversorgung getrennt werden, sonst besteht die Gefahr, daß sowohl die Grundgeräte als auch die Erweiterungskarte zerstört werden.

- Ziehen Sie immer den Netzstecker von **X4100/200/300** und alle Verbindungsleitungen der Erweiterungskarte, bevor Sie die Erweiterungskarte einstecken oder austauschen.
- Schließen Sie **X4100/200/300** erst an die Stromversorgung an, nachdem das Gerät vollständig verschlossen ist und Sie die Installation noch mal geprüft haben.

Gefahr!

Fassen Sie beim Einbau oder Austausch der Erweiterungskarte nicht in den Erweiterungssteckplatz. Es besteht Lebensgefahr durch Stromschlag!

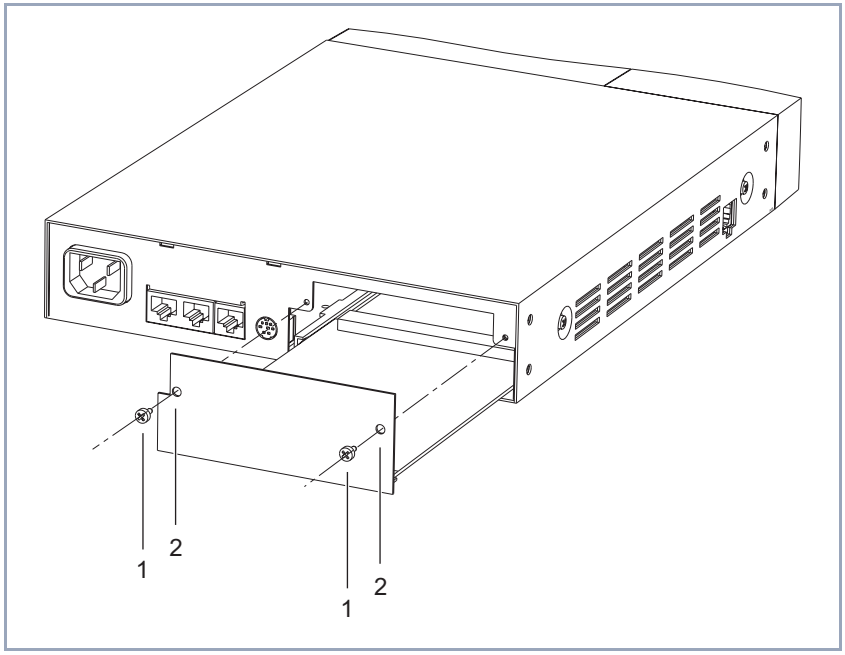
- Fassen Sie nicht in den Erweiterungssteckplatz von **X4100/200/300**!

Achtung!

Elektrostatische Aufladung kann elektronische Bauteile schädigen. Um die Schädigung von Bauteilen zu vermeiden, beachten Sie bitte folgende Vorsichtsmaßnahmen:

- Erden Sie sich, bevor Sie Bauteile auspacken und bevor Sie Installationsarbeiten am Gerät durchführen.
- Berühren Sie Platinen immer nur an den Rändern, und fassen Sie nicht auf Leitungen oder Bauteile.

Grafische Darstellung der Installation einer Erweiterungskarte:



1	Schraube zum Befestigen der Erweiterungskarte	2	Bohrung zum Befestigen der Erweiterungskarte

Bild 3-11: Installation einer Erweiterungskarte am Beispiel **X4100**

Einbau/Austausch

Gehen Sie folgendermaßen vor, um eine Erweiterungskarte einzubauen bzw. auszutauschen:

Achtung!

Der Einbau der PRI/G.703-Erweiterungskarte führt zu verstärkter Wärmeentwicklung. Um die Schädigung von Bauteilen zu vermeiden, ist der Einsatz einer Lüfterkassette zwingend erforderlich!

➤ Setzen Sie bei Verwendung der PRI/G.703-Erweiterungskarte im **X4100/200/300**-Einbaugerät die Lüfterkassette ein.

Sie können die Lüfterkassette von Ihrem Lieferanten käuflich erwerben.

- Lösen Sie die Schrauben der Blindabdeckung oder der eingebauten Erweiterungskarte.
- Nehmen Sie die Blindabdeckung ab bzw. ziehen Sie die vorhandene Erweiterungskarte heraus.
  Behalten Sie die beiden Schrauben der Blindabdeckung für die Befestigung der Erweiterungskarte.
- Montieren Sie gegebenenfalls die Ressourcenkarte(n) auf der Erweiterungskarte.
  Beachten Sie dazu die im Lieferumfang der Ressourcenkarte enthaltene Einbauanleitung.
- Stecken Sie die einzubauende Erweiterungskarte in den dafür vorgesehenen Steckplatz des Gehäuses, bis sie in den Steckverbinder des Steckplatzes eingerastet ist.
  Kartenführungen ermöglichen ein sicheres Stecken der Erweiterungskarte.
- Nachdem die Erweiterungskarte eingerastet ist, befestigen Sie sie mit den beiden Schrauben, die Sie zuvor von der Blindabdeckung gelöst oder von der auszutauschenden Erweiterungskarte behalten haben (siehe Bild 3-11, Seite 44), am Gehäuse.

Achtung!

Der Einbau von Ressourcenkarten in eine Erweiterungskarte führt zu verstärkter Wärmeentwicklung. Um die Schädigung von Bauteilen zu vermeiden, ist der Einsatz einer Lüfterkassette zwingend erforderlich!

- Setzen Sie bei Verwendung einer Erweiterungskarte mit Ressourcenkarte(n) im **X4100/200/300**-Einbaugerät die Lüfterkassette ein.

Sie können die Lüfterkassette von Ihrem Lieferanten käuflich erwerben.

Ausbau Zum Ausbau einer Erweiterungskarte führen Sie die zuvor beschriebenen Installationsschritte in umgekehrter Reihenfolge durch.

3.4 Aufstellen und Anschließen

Die Beschreibung der Anschlüsse von **X4100/200/300** finden Sie in Kapitel 3.1.2, Seite 33.

Achtung!

Bei falscher Verkabelung der ISDN- und LAN-Schnittstellen kann es zu einem Defekt an Ihrem Router kommen.

- Verbinden Sie immer nur die LAN-Schnittstelle von **X4100/200/300** mit der LAN-Schnittstelle des Hubs und die ISDN-Schnittstelle von **X4100/200/300** mit dem ISDN-Anschluß.

Gehen Sie beim Anschließen in folgender Reihenfolge vor:

- Stellen Sie **X4100/200/300** auf eine feste, ebene Unterlage.

X4100/200/300 an PC oder Terminal anschließen

- Verbinden Sie die serielle Schnittstelle Ihres Rechners (COM1 oder COM2) mit der Konsolenschnittstelle von **X4100/200/300**. Verwenden Sie dazu das mitgelieferte serielle Kabel.
  Das Anschließen von **X4100/200/300** an die Konsolenschnittstelle (5, siehe Bild 3-2, Seite 33, Bild 3-3, Seite 34 und Bild 3-4, Seite 35) ist nur dann erforderlich, wenn Sie Ihre Initialkonfiguration über den Konsolen-Port seriell vornehmen möchten, z. B. HyperTerminal.

Wenn Sie **X4100/200/300** nur die IP-Adresse und Netzmaske zuweisen wollen, ist keine serielle Verbindung erforderlich. Das Zuweisen der IP-Adresse können Sie schnell und einfach mit MMI vornehmen (MMI, Kapitel 5, Seite 83).

X4100/200/300 an LAN anschließen

- Verbinden Sie die LAN-Schnittstelle (3, siehe Bild 3-2, Seite 33, Bild 3-3, Seite 34 und Bild 3-4, Seite 35) von **X4100/200/300** mit Ihrem Hub. Verwenden Sie dazu nur CAT5-taugliche LAN-Kabel. Eine schlechtere Kabelqualität kann zu Fehlfunktionen von **X4100/200/300** führen.

X4100/200/300 an WAN anschließen

Wenn Sie in Ihrem Anwendungsszenario die ISDN-BRI-Schnittstelle verwenden wollen:

- Verbinden Sie die ISDN-BRI-Schnittstelle (2, siehe Bild 3-2, Seite 33, Bild 3-3, Seite 34 und Bild 3-4, Seite 35) von **X4100/200/300** über das mitgelieferte Kabel (RJ-45) mit Ihrem ISDN-Anschluß.

Wenn Sie in Ihrem Anwendungsszenario die 10-Base-T-Ethernet-für-xDSL-Schnittstelle (**X4100** und **X4200**) bzw. X.21/V.35-Schnittstelle(n) (**X4200** und **X4300**) verwenden wollen:

➤ Verbinden Sie die 10-Base-T-Ethernet-für-xDSL-Schnittstelle bzw. X.21/V.35-Schnittstelle (4 bzw. 8, siehe Bild 3-2, Seite 33, Bild 3-3, Seite 34 und Bild 3-4, Seite 35) von **X4100/200/300** über ein Anschlußkabel (nicht im Lieferumfang enthalten!) mit ihrem Anschluß.

Wir empfehlen, original BinTec-Kabel zu verwenden, die Sie von Ihrem Händler beziehen können.

Die Verwendung von anderen Kabeln kann zur Beschädigung des Geräts und damit zum Garantieverlust führen!

Erweiterungskarte

Wenn Sie Ihre Erweiterungskarte anschließen wollen:

➤ Stecken Sie die benötigten Schnittstellenkabel Ihrer Erweiterungskarte in die dafür vorgesehenen Buchsen.

Bei der PRI/G.703-Erweiterungskarte stehen pro Schnittstelle zwei RJ45-Buchsen zur Verfügung – IN und OUT.

Beim Anschließen der Erweiterungskarte verbinden Sie das Anschlußkabel mit der IN-Buchse. Über die OUT-Buchse können Sie optional einen Backup-Router anschließen, der beim Abschalten oder Ausfallen des ersten Routers dessen Funktion übernehmen kann.

X4100/200/300 an die Stromversorgung anschließen

➤ Schließen Sie **X4100/200/300** über das mitgelieferte Kaltgerätenetzkabel an eine Steckdose bzw. an die Stromversorgung des 19-Zoll-Schranks an.

X4100/200/300-Selbsttest

X4100/200/300 führt einen Selbsttest durch, siehe auch Kapitel 3.6, Seite 52. Wenn Sie alle Kabel richtig angeschlossen haben, erlöschen am Ende des Selbsttests die rote LED der C-Taste am Display sowie die rote LED auf der Rückseite des Gerätes.

Die Statusmeldungen, die über Leuchtdioden (LEDs) angezeigt werden, finden Sie in Kapitel 3.5, Seite 49.

Hardware-Grundeinstellungen

➤ Nehmen Sie über Tastatur und Display die erforderlichen Hardware-Grundeinstellungen vor (eine detaillierte Beschreibung finden Sie in Kapitel 5, Seite 83):

– Dialogsprache im MMI auswählen.

– IP-Adresse und Netzmaske eingeben, damit die weitere Konfiguration über das LAN erfolgen kann und nicht über den Konsolen-Port durchgeführt werden muß.

3.5 Statusmeldung über Leuchtdioden (LEDs)

Im folgenden werden die verschiedenen LED-Arten vorgestellt, über die das **X4100/200/300**-Grundgerät Statusmeldungen abgeben kann, und die Bedeutung der LEDs auf den Erweiterungskarten.

3.5.1 Grundgerät

Beleuchtete Eingabetasten

Die während der Bedienung beleuchteten Eingabetasten des Displays führen Sie durch das MMI.

Eine detaillierte Beschreibung der LEDs des MMI finden Sie in Kapitel 5.2.2, Seite 87.

Grundsätzlich zeigt das Blinken oder Leuchten der grünen LED einen störungsfreien Betrieb an, während das Blinken oder Leuchten der roten LED auf eine Störung hinweist.

Detailliertere Statusinformationen erhalten Sie über das Display, das Setup Tool oder ein SNMP-Management-Tool.

3.5.2 Erweiterungskarten

Die Erweiterungskarten sind mit Leuchtdioden ausgestattet. Die Statusmeldungen dieser Leuchtdioden bei gesteckten Anschlußkabeln werden in diesem Kapitel erläutert.

BRI-Erweiterungskarte X4E-2/3BRI

Die BRI-Erweiterungskarte verfügt über sechs LEDs, jeweils zwei LEDs (gelb und grün) sind einem Port zugeordnet.

Die LEDs der BRI-Erweiterungskarte zeigen folgende Statusmeldungen an:

	LED leuchtet	LED blinkt	Bedeutung
grüne LED	X	–	1 B-Kanal wird genutzt
	–	X	2 B-Kanäle werden genutzt
	–	–	Keiner der B-Kanäle wird genutzt
gelb LED	X	–	D-Kanal fehlt oder Autokonfiguration schlug fehl
	–	X	Schicht 1 nicht stabil

Tabelle 3-1: LED-Statusmeldungen einer BRI-Erweiterungskarte

PRI/G.703-Erweiterungskarte X4E-1/2PRI

Die PRI/G.703-Erweiterungskarte verfügt über zwei LEDs. Die obere ist dem ersten Port zugeordnet (Unit 0), die untere dem zweiten Port (Unit 1).

Die LEDs der PRI/G.703-Erweiterungskarte zeigen folgende Statusmeldungen an:

LED leuchtet	LED blinkt	Bedeutung
–	–	Port ist nicht per Lizenz freigeschaltet
X	–	Port befindet sich im G.703-Modus (Lizenz für G.703 oder PRI ist aktiviert und unter **ISDN Line Framing** ist *G.703* ausgewählt)
–	X	Port befindet sich im PRI-Modus (Lizenz für PRI ist aktiviert und unter **ISDN Line Framing** ist nicht *G.703* ausgewählt)

Tabelle 3-2: LED-Statusmeldungen einer PRI/G.703-Erweiterungskarte

LAN-Erweiterungskarte X4E-2FE

Die LAN-Erweiterungskarte verfügt über 4 LEDs. Die beiden LEDs auf der linken Seite (rot und grün) sind dem ersten Port zugeordnet (Unit 0), die beiden LEDs auf der rechten Seite (rot und grün) dem zweiten Port (Unit 1).

Die roten LEDs der LAN-Erweiterungskarte leuchten bei Ethernet-Kollisionen auf, die grünen LEDs zeigen die Aktivität auf dem Ethernet an:

	LED blinkt	LED leuchtet	Bedeutung
grüne LED	–	X	100 MBit/s-Modus (Fast Ethernet)
	X	–	10 MBit/s-Modus (Ethernet)
	–	–	Port ist nicht verfügbar
rote LED	–	X	Ethernet-Kollision
	–	–	keine Ethernet-Kollision

Tabelle 3-3: Statusmeldungen der LEDs einer LAN-Erweiterungskarte

3.6 Boot-Sequenz

Beim Hochfahren durchläuft **X4100/200/300** verschiedene Funktionszustände:

- Start-Modus
- BOOTmonitor-Modus
- Normaler Betriebs-Modus

Nachdem im Start-Modus einige Selbsttests erfolgreich ausgeführt wurden, erreicht **X4100/200/300** den BOOTmonitor-Modus. Der BOOTmonitor-Prompt wird angezeigt, falls Sie seriell mit **X4100/200/300** verbunden sind.

BOOTmonitor

Betätigen Sie nach Anzeige des BOOTmonitor-Prompts innerhalb von vier Sekunden die **Leertaste**, um die Funktionen des BOOTmonitors zu nutzen. Wenn Sie keine Eingabe machen, wechselt **X4100/200/300** nach Ablauf der vier 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:
  X4100/200/300 lädt die komprimierte Boot-Datei vom Flash-Speicher in den Arbeitsspeicher. Dies wird beim Hochfahren automatisch ausgeführt.
- (2) Software Update via TFTP:
  X4100/200/300 führt ein Software-Update über einen TFTP-Server aus.
- (3) Software Update via XMODEM:
  X4100/200/300 führt ein Software-Update über eine serielle Schnittstelle mit XMODEM aus.
- (4) Delete Configuration:
  X4100/200/300 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 des BOOTmonitors von **X4100/200/300** verändern, z. B. die Baudrate für serielle Verbindungen.

- (6) Show system information:
  Zeigt nützliche Informationen von **X4100/200/300**, wie z. B. Seriennummer, MAC-Adresse und Software-Versionen.

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 **X4100/200/300** herstellen!

4 Voraussetzungen für die Konfiguration

In diesem Kapitel erläutert folgendes:

- Wie Sie auf **X4100/200/300** zugreifen (Kapitel 4.1, Seite 56)
- Wie Sie sich auf **X4100/200/300** anmelden (Kapitel 4.2, Seite 62)
- Welche Konfigurationsmöglichkeiten Ihnen zur Verfügung stehen (Kapitel 4.3, Seite 64)
- Wie das ➤➤ **Setup Tool** aufgebaut ist (Kapitel 4.4, Seite 66)
- Wie Sie bei einer Initialkonfiguration von **X4100/200/300** vorgehen sollten (Kapitel 4.5, Seite 78)

4.1 Zugangsmöglichkeiten

Für den Zugriff auf **X4100/200/300** zur Konfiguration gibt es verschiedene Möglichkeiten:

- Über das Man Machine Interface (MMI)
- Über die serielle Schnittstelle
- Über Ihr ➤➤ **LAN**
- Über eine ➤➤ **ISDN**-Verbindung

Hier eine grafische Darstellung der Zugangsmöglichkeiten:

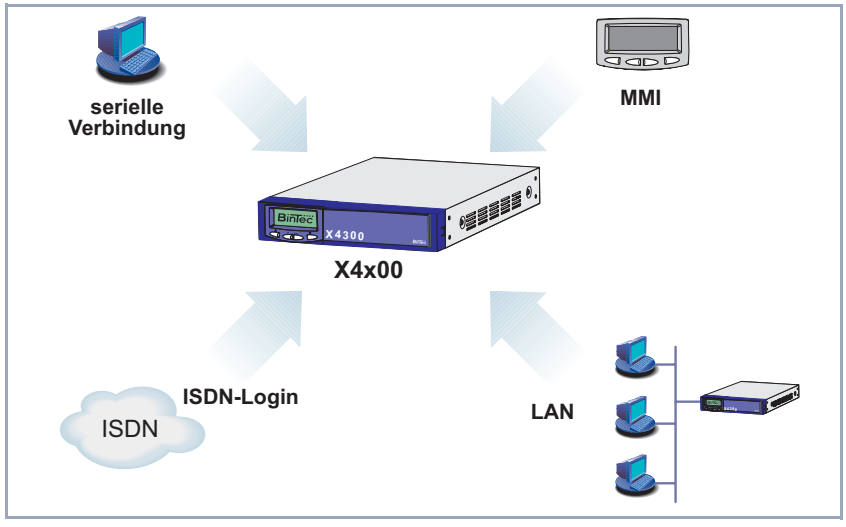


Bild 4-1: Zugangsmöglichkeiten zu **X4100/200/300**

Im folgenden werden die verschiedenen Zugangsmöglichkeiten vorgestellt. Wählen Sie das für Ihre Bedürfnisse geeignete Vorgehen.

4.1.1 Man Machine Interface (MMI)

Erste Schritte

Das MMI mit Display und Eingabetasten ist eine gute Möglichkeit, um einen "ersten Kontakt" zu **X4100/200/300** herzustellen. Mit dem MMI sollten Sie folgende erste Schritte durchführen (siehe Kapitel 5, Seite 83):

- gewünschte Display-Sprache einstellen
- IP-Adresse und Netzmaske eintragen

Die weiteren Konfigurationsschritte führen Sie dann mit dem Setup Tool durch.

4.1.2 Zugang über die serielle Schnittstelle

Erstkonfiguration

Der Zugang über die serielle Schnittstelle ist gut geeignet, wenn Sie bei **X4100/200/300** eine Initialkonfiguration durchführen und noch keine IP-Adresse und Netzmaske eingetragen haben. Um **X4100/200/300** über die serielle Schnittstelle an Ihren Rechner anzuschließen, verbinden Sie die serielle Schnittstelle am Grundgerät der **X4100/200/300** mit der seriellen Schnittstelle Ihres Rechners.

Windows

Wenn Sie einen Windows-PC benutzen, benötigen Sie für die serielle Verbindung ein Terminal-Programm, z. B. **HyperTerminal**. Wie Sie dieses Hilfsprogramm und die **BRICKware for Windows** installieren, finden Sie in Kapitel 4.5.2, Seite 80.

Gehen Sie folgendermaßen vor, um über die serielle Schnittstelle auf **X4100/200/300** zuzugreifen:

ToDo

- Klicken Sie im Windows-Startmenü auf **Programme** ➧ **BRICKware** ➧ **Gerät an COM1** (bzw. **Gerät an 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 öffnet sich ein Fenster mit dem Login-Prompt. Sie befinden sich auf der SNMP-Shell von **X4100/200/300**.
- Fahren Sie fort mit Kapitel 4.2, Seite 62.

Falls der Login-Prompt auch nach mehrmaligem Betätigen der **Eingabetaste** nicht erscheint, konnte die Verbindung zu **X4100/200/300** nicht hergestellt werden. Überprüfen Sie daher die Einstellungen von COM1 bzw. COM2 Ihres Rechners:

- Klicken Sie auf **Datei** ➧ **Eigenschaften**.
- Klicken Sie im Register **Verbinden mit** auf **Konfigurieren**....
  Folgende Einstellungen sind erforderlich:
  - Bits per second: 9600
  - Data bits: 8
  - Parity: None
  - Stopbits: 1
  - Flow Control: None
- Tragen Sie die Werte ein und klicken Sie auf **OK**.
- Stellen Sie im Register **Einstellungen** ein:
  - Emulation: VT100
- Klicken Sie auf **OK**.

Damit Änderungen an den Terminal-Programmeinstellungen wirksam werden, müssen Sie die Verbindung zu **X4100/200/300** trennen und sich wieder neu verbinden.

Sie können auch jedes andere Terminal-Programm verwenden, das sich auf 9600 bit/s, 8N1 (8 Datenbits, No Parity, 1 Stopbit), Softwarehandshake (none) und VT100-Emulation einstellen läßt.

Unix Sie benötigen ein Terminal-Programm wie z. B. `cu` (unter System V), `tip` (unter BSD) oder `minicom` (unter Linux). Die Einstellungen für diese Programme entsprechen den oben aufgelisteten.

Beispiel für eine Befehlszeile, um `cu` zu nutzen: `cu -s 9600 -c/dev/ttyb`

Beispiel für eine Befehlszeile, um `tip` zu nutzen: `tip -9600 /dev/ttyb`

4.1.3 Zugang über LAN

Über den Dienst ➤➤ **Telnet** können Sie **X4100/200/300** vom LAN aus erreichen. Telnet steht normalerweise auf jedem Rechner zur Verfügung. Um **X4100/200/300** über das LAN erreichen zu können, muß der Router bereits eine ➤➤ **IP-Adresse** und ➤➤ **Netzmaske** haben. Wenn dies nicht der Fall ist, **X4100/200/300** also noch unkonfiguriert ist, haben Sie zwei Möglichkeiten:

- Geben Sie IP-Adresse und Netzmaske über die Eingabetasten des MMI ein (siehe Kapitel 5, Seite 83).
- Wenn Sie mit Windows arbeiten, können Sie **X4100/200/300** eine IP-Adresse zuweisen, indem Sie das Hilfsprogramm ➤➤ **DIME Tools** verwenden. Wenn Sie **DIME Tools** zusammen mit der **BRICKware for Windows** noch nicht installiert haben, gehen Sie vor wie in Kapitel 4.5.2, Seite 80 beschrieben.

ToDo

Gehen Sie folgendermaßen vor, um über das LAN auf **X4100/200/300** zuzugreifen:

➤ Schließen Sie **X4100/200/300** an das LAN an.

IP-Adresse zuweisen

Gehen Sie folgendermaßen vor, um **X4100/200/300** mit dem Programm **DIME Tools** eine IP-Adresse zuzuweisen (falls dies nötig ist):

➤ Klicken Sie im Windows-Startmenü auf **Programme** ➧ **BRICKware** ➧ **DIME Tools**.
Wenn der ➤➤ **BootP**-Server nicht automatisch gestartet ist, starten Sie ihn manuell.

Nach kurzer Zeit öffnet sich das BootP-Server-Fenster, wenn **X4100/200/300** noch unkonfiguriert ist.

➤ Geben Sie in dem Fenster unter **Device Parameter** Name und IP-Adresse von **X4100/200/300** ein.

➤ Klicken Sie auf **OK**.

➤ Schließen Sie **DIME Tools**.

Telnet ausführen

Bauen Sie nun mit Telnet eine Verbindung zu **X4100/200/300** auf:

Windows

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

- Geben Sie `telnet <IP-Adresse von` **X4100/200/300**> ein.
- Klicken Sie auf **OK**.

  Es öffnet sich ein Fenster mit dem Login-Prompt. Sie befinden sich auf der SNMP-Shell von **X4100/200/300**. Fahren Sie fort mit Kapitel 4.2, Seite 62.

Unix

- Geben Sie `telnet <IP-Adresse von` **X4100/200/300**> in ein Terminal ein.

  Es erscheint ein Fenster mit dem Login-Prompt. Sie befinden sich auf der SNMP-Shell von **X4100/200/300**. Fahren Sie fort mit Kapitel 4.2, Seite 62.

4.1.4 Zugang über ISDN

Remote-Konfiguration

Der Zugang über ➤➤ **ISDN** mit ➤➤ **ISDN-Login** empfiehlt sich vor allem dann, wenn **X4100/200/300** aus der Ferne (Remote-LAN in Bild 4-2, Seite 61) konfiguriert oder gewartet werden soll. Dies ist auch dann möglich, wenn **X4100/200/300** sich noch im Auslieferungszustand befindet. Der Zugang erfolgt dann mit Hilfe eines bereits konfigurierten BinTec-Routers oder einer ISDN-Karte im Remote-LAN unter Benutzung einer Rufnummer des ISDN-Anschlusses von **X4100/200/300** im eigenen LAN (z. B. 1234).

So kann z. B. der Administrator im Remote-LAN **X4100/200/300** konfigurieren, ohne vor Ort zu sein. **X4100/200/300** in Ihrem LAN muß lediglich mit dem ISDN-Anschluß verbunden und eingeschaltet sein.

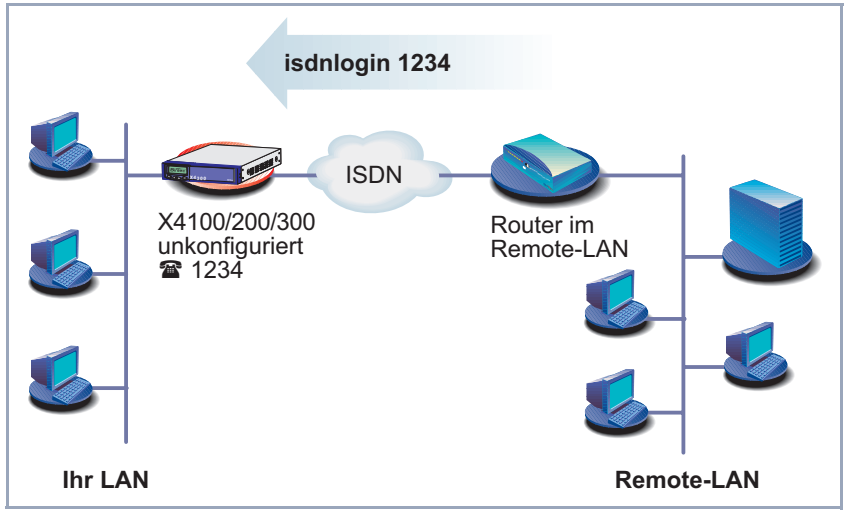


Bild 4-2: Zugang über ISDN-Login für Fernwartung

Der Zugang über ISDN verursacht Kosten. Wenn **X4100/200/300** und Rechner im gleichen LAN sind, ist es billiger, auf **X4100/200/300** über das LAN oder über die serielle Schnittstelle zuzugreifen.

ToDo Gehen Sie folgendermaßen vor, um **X4100/200/300** über ISDN-Login zu erreichen:

- Schließen Sie **X4100/200/300** an ISDN an.
- Loggen Sie sich wie gewohnt auf Ihrem BinTec-Router im Remote-LAN ein.
- Geben Sie in der SNMP-Shell `isdnlogin <Rufnummer des ISDN-Anschlusses von X4100/200/300>` ein, z. B. `isdnlogin 1234`.

Es erscheint der Login-Prompt. Sie befinden sich auf der SNMP-Shell von **X4100/200/300**. Fahren Sie fort mit Kapitel 4.2, Seite 62.

4.2 Anmelden

Unabhängig davon, über welchen Weg Sie auf **X4100/200/300** zugreifen, erscheint zunächst die ➤➤ **SNMP-Shell** von **X4100/200/300** mit dem Login-Prompt. Eine Ausnahme bilden hier der **Configuration Manager** unter Windows und das MMI.

4.2.1 Benutzername und Paßwörter im Auslieferungszustand

Um sich anmelden zu können, müssen Sie Benutzernamen und Paßwort kennen. Im Auslieferungszustand ist **X4100/200/300** 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 **X4100/200/300** verloren).
`read`	public	Systemvariablen lesen.

Tabelle 4-1: Benutzernamen und Paßwörter im Auslieferungszustand

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

4.2.2 Einloggen

Zugangsdaten (Benutzernamen und Paßwörter) sind auch nur dann änderbar, wenn sich der Benutzer `admin` einloggt. Aus Sicherheitsgründen sind Paßwörter im Setup Tool im Auslieferungszustand nicht im Klartext, sondern nur als Sternchen am Bildschirm sichtbar. Die Benutzernamen erscheinen hingegen

im Klartext. Durch das Sicherheitskonzept von **X4100/200/300** können Sie 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.

ToDo 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. `X4000:>`. Das Einloggen war erfolgreich.

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. Die Vorgehensweise bei der Änderung von Paßwörtern ist unter Kapitel 4.4.4, Seite 71 beschrieben.

- Ändern Sie unbedingt die Paßwörter, um unberechtigten Zugriff auf **X4100/200/300** zu verhindern.
- Merken Sie sich Ihr Paßwort!
  Haben Sie ihr Paßwort vergessen, dann müssen Sie **X4100/200/300** in den Auslieferungszustand zurückversetzen und Ihre Konfiguration geht verloren!

Die Befugnisse der Benutzernamen und Paßwörter finden Sie in Kapitel 4.2.1, Seite 62.

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

4.3 Konfigurationsmöglichkeiten

Bevor Sie mit der Konfiguration beginnen, 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 **X4100/200/300** konfigurieren.

Übersicht Die Möglichkeiten, **X4100/200/300** zu konfigurieren:

- MMI (Man Machine Interface)
- Setup Tool
- ➤➤ **SNMP**-Shell-Kommandos
- **Configuration Manager** und andere SNMP-Manager

MMI Mit dem einfach zu bedienenden und selbsterklärenden Man Machine Interface (MMI) haben Sie die Möglichkeit, Informationen über **X4100/200/300** auf dem Display anzuzeigen. Sie können außerdem grundlegende Einstellungen wie z. B. IP-Adresse und Netzmaske über die Eingabetasten vornehmen. Eine umfassende Konfiguration ist mit dem MMI nicht möglich. Dafür sollten Sie das Setup Tool verwenden. Detaillierte Informationen zum MMI und die komplette Menüstruktur finden Sie in Kapitel 5, Seite 83.

Setup Tool Das Setup Tool ist ein menügesteuertes Tool zur Konfiguration und Administration von **X4100/200/300**. 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 das Setup Tool zur Konfiguration beschrieben. Das Setup Tool ist unabhängig vom Betriebssystem Ihres Rechners. 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.

Configuration Manager und andere SNMP-Manager

Mit dem **Configuration Manager** stellt BinTec Access Networks GmbH einen Windows-basierten SNMP-Manager zur Verfügung. In einer an den Windows-Explorer angelehnten Oberfläche können Sie damit auf alle MIB-Tabellen und -Variablen von **X4100/200/300** 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 Zusammenhänge der Tabellen und Subsysteme von **X4100/200/300** erforderlich, die Methode ist also für erfahrene Nutzer interessant. In diesem Handbuch wird der Umgang mit MIB-Tabellen und MIB-Variablen nicht erläutert. Sie finden diese in der **Software Reference** und **MIB Reference**.

4.4 Bedienung des Setup Tools

Wenn Sie sich auf **X4100/200/300** 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 öffnet sich.

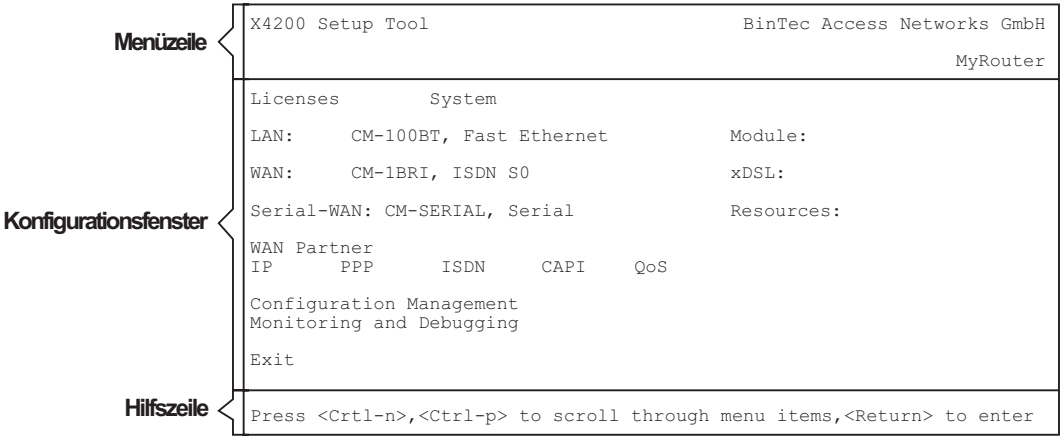


Bild 4-3: Erläuterung der Setup-Tool-Menüs am Beispiel **X4200**

Für das Grundgerät **X4100** entfällt der Menüpunkt **Serial-WAN** und für das Grundgerät **X4300** entfällt der Menüpunkt **xDSL**.

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 4.2, Seite 62).

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 der **X4100/200/300**.

Setup-Tool-Menü

Jedes Setup-Tool-Menü besteht aus drei Bereichen (siehe Bild 4-3, Seite 66):

- In der Menüzeile befindet sich eine Navigationshilfe, die anzeigt, in welchem Menü des Setup Tools Sie sich gerade befinden. Zusätzlich wird der Systemname von **X4100/200/300** 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.

4.4.1 Menünavigation

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** (Pfeiltasten, nicht unter Windows 2000)	Zum nächsten und vorherigen Feld im Menü springen (arbeitet mit VT 100-Emulation bei Verwendung eines Terminal-Programms).
left und **right** (Pfeiltasten, nicht unter Windows 2000)	Vorherige und nachfolgende Werte von Feldern sichtbar machen (arbeitet mit VT 100-Emulation bei Verwendung eines Terminal-Programms).
Esc Esc	Zweimal nacheinander **Esc**: Zum vorherigen Menü zurückkehren. Veränderungen gehen verloren.

Tastenkombination	Bedeutung
Leertaste	Listeneinträge 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 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 Liste, die nicht vollständig angezeigt wird, nach oben blättern. Rechts oben zeigt ein "=" den Anfang der Liste bzw. ein "∧" weitere Listeneinträge an.
Strg - **c**	Setup Tool verlassen.

Tabelle 4-2: Navigation im Setup Tool

4.4.2 Menükommandos

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 öffnet sich, in dem Sie die gewünschten Einstellungen eintragen.
CANCEL	Alle Änderungen in dem gerade angezeigten Menü löschen.

Schaltfläche	Bedeutung
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 4-3: Schaltflächen im Setup Tool

Zum Speichern der Konfiguration im Flash ist es notwendig, das Setup Tool mit **Save as boot configuration and exit** zu verlassen.

4.4.3 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:

```
X4x00 Setup Tool                              BinTec Access Networks GmbH
[WAN]: WAN Partners                                              MyRouter


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>toedit
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**.

Achten Sie darauf, daß sich der Cursor auf einem Listen-Element befindet. Die Suche kann nicht ausgeführt werden, wenn sich der Cursor auf einem Kommandofeld, 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 4-4: Suchergebnisse

4.4.4 Paßwortänderung

Die im folgenden beschriebene Vorgehensweise zur Paßwortänderung betrifft alle Paßwörter auf **X4100/200/300**: die Zugangspaßwörter für die Benutzernamen `admin`, `read` und `write`, das RADIUS-Paßwort, das PPP-Paßwort, das Provider-Paßwort und die CAPI-Benutzer-Paßwörter.

Es dürfen alle Zeichen zur Eingabe eines Paßworts verwendet werden. Angezeigt werden Paßwörter – auch bei der Paßwortänderungen – nur als Sternchen. Die Zahl der Sternchen stimmt mit der Zeichenzahl des Paßworts überein.

Um das Setup Tool von **X4100/200/300** in einem Modus zu starten, in dem die Paßwörter im Klartext angezeigt werden und durch einmaliges Editieren geändert werden können, müssen Sie den Befehl `setup -p` eingeben. Diese Möglichkeit besteht nur für einen Benutzer, der mit dem Benutzernamen `admin` auf **X4100/200/300** eingeloggt ist.

Paßwort ändern Um ein Paßwort zu ändern, gehen Sie folgendermaßen vor:

Im Paßwortfeld löscht die Taste **Backspace** immer die gesamte Eingabe, nicht nur ein Zeichen.

- Selektieren Sie das Paßwortfeld und geben Sie das neue Paßwort ein.
  Das Feld wechselt in den Änderungsmodus und in der Hilfszeile erscheint die Meldung `Change Password`.
- Bestätigen Sie nun mit der **Eingabetaste**, dem **Tabulator** oder einer **Cursortaste**.
  Das Feld wechselt in den Bestätigungsmodus und in der Hilfszeile wird `Confirm Password` angezeigt.
- Geben Sie nun erneut das neue Paßwort ein und bestätigen Sie die Eingabe mit der **Eingabetaste**, dem **Tabulator** oder einer **Cursortaste**.
  Wurde das Paßwort das zweite Mal fehlerfrei eingeben, wird das Paßwort geändert und nach dem Verlassen des Menüs mit der Schaltfläche **SAVE** gespeichert. Verlassen Sie das Menü mit **CANCEL** oder **Esc Esc**, wird die Paßwortänderung nicht gespeichert.
  Waren beide Angaben ungleich, wird das Feld auf das alte Paßwort zurückgesetzt und in der Hilfszeile wird die Meldung: "`Password doesn't match. Try again.`" angezeigt.

4.4.5 Menüstruktur

Das Hauptmenü des Setup Tools sieht folgendermaßen aus:

```
X4x00 Setup Tool                                BinTec Access Networks GmbH
                                                                  MyRouter

Licenses                 System

LAN:         CM-100BT, Fast Ethernet           Module:

WAN:         CM-1BRI, ISDN S0                  xDSL:

Serial-WAN:  CM-SERIAL, Serial                 Resources:

WAN Partner
IP      PPP      ISDN     CAPI     QoS

Configuration Management
Monitoring and Debugging
Exit

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

Die auf **X4100/200/300** zur Verfügung stehenden Menüs des Setup Tools sind in Bild 4-4, Seite 74 dargestellt. Wenn Sie die erforderliche Lizenz aktivieren, erkennt **X4100/200/300** dies und zeigt die entsprechenden Menüs an (Lizenz eintragen siehe Kapitel 6.1.1, Seite 102).

Für das Grundgerät **X4100** entfällt der Menüpunkt **Serial-WAN** und für das Grundgerät **X4300** entfällt der Menüpunkt **xDSL**.

Die Menüstruktur (Hauptmenü und erste Untermenüs) des Setup Tools sieht folgendermaßen aus:

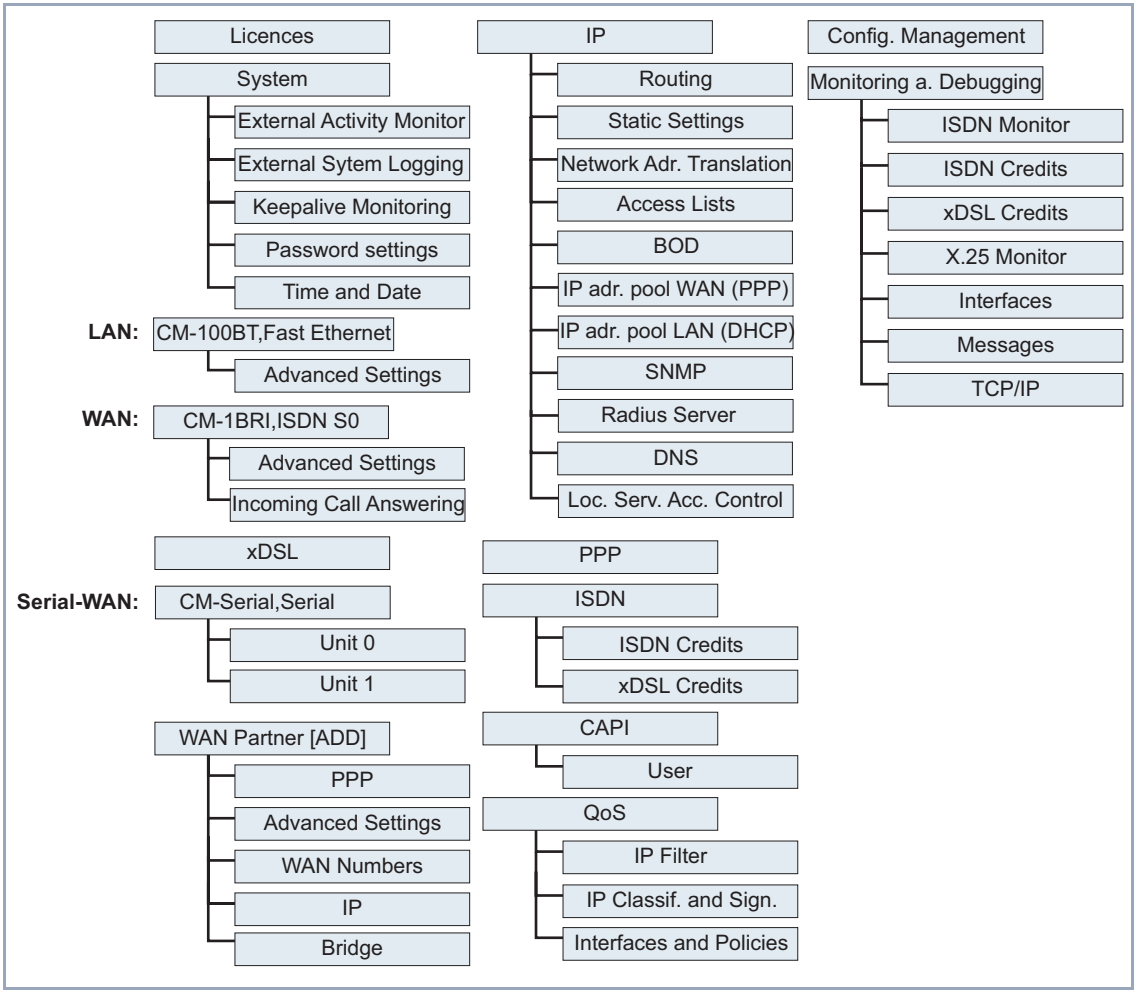


Bild 4-4: Setup Tool Menüstruktur (Grundgerät)

Überblick

Um die Orientierung bei der Konfiguration zu erleichtern, werden die Menüs kurz erläutert:

Menü	Funktion
LICENSES	In diesem Menü tragen Sie die Lizenzinformationen ein. Hier aktivieren Sie die Zusatzlizenzen.
SYSTEM	In diesem Menü tragen Sie die grundlegenden Systemeinstellungen von **X4100/200/300** ein, wie z. B. Systemname und Paßwörter.
FAST ETHERNET	In diesem Menü konfigurieren Sie die ➤➤ **LAN**-Schnittstelle von **X4100/200/300**. Hier tragen Sie z. B. die IP-Adresse und Netzmaske des Gerätes ein.
ISDN S0	In diesem Menü konfigurieren Sie die ISDN-Schnittstelle von **X4100/200/300**. Hier tragen Sie z. B. ein, an welcher Art von ISDN-Anschluß **X4100/200/300** angeschlossen ist. Im Untermenü ***ISDN S0*** ➧ ***INCOMING CALL ANSWERING*** teilen Sie die zur Verfügung stehenden ISDN-Rufnummern den gewünschten Diensten (z. B. PPP-Routing, ➤➤ **CAPI**, ➤➤ **ISDN-Login**) zu.
xDSL	In diesem Menü konfigurieren Sie die 10-BT-Ethernet-Schnittstelle für xDSL-Verbindungen (nur **X4100** und **x4200**).
SERIAL	In diesem Menü konfigurieren Sie die seriellen WAN-Schnittstellen von (nur **X4200 und X4300**).
WAN PARTNER	In diesem Menü definieren Sie alle WAN-Partner, z. B. Ihren ➤➤ **Internet** Service Provider (➤➤ **ISP**). 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 alle Einstellungen ein, die das ➤➤ **IP**-Protokoll betreffen. Es besteht aus mehreren Untermenüs: ***IP*** ➧ ***ROUTING*** enthält die IP-Routing-Tabelle von **X4100/200/300**. Hier tragen Sie Routen zu Ihren Partnern ein (z. B. Default-Routen, Netzwerk-Routen), damit das Gerät alle ➤➤ **Datenpakete** an die richtigen Adressen weiterleitet. In ***IP*** ➧ ***STATIC SETTINGS*** tragen Sie einige wichtige Einstellungen ein, z. B. den Domain-Namen von **X4100/200/300**, 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 **X4100/200/300** ungewollt Verbindungen zum ISDN aufbaut. In ***IP*** ➧ ***BANDWIDTH ON DEMAND (BOD)*** definieren Sie Filter für die Funktion "Bandwidth on Demand" bzw. AO/DI (Always On/Dynamic ISDN). In ***IP*** ➧ ***IP ADDRESS POOL WAN (PPP)*** können Sie einen Pool von IP-Adressen einrichten, die **X4100/200/300** als dynamischer IP-Address-Server an WAN-Partner vergibt, die sich einwählen. In ***IP*** ➧ ***IP ADDRESS POOL LAN (DHCP)*** konfigurieren Sie **X4100/200/300** als ➤➤ **DHCP**-Server. Als DHCP-Server teilt **X4100/200/300** Hosts im LAN deren IP-Adressen dynamisch zu. In ***IP*** ➧ ***SNMP*** können Sie die grundlegenden ➤➤ **SNMP**-Einstellungen ändern. In ***IP*** ➧ ***RADIUS SERVER*** legen Sie den RADIUS-Server fest. In ***IP*** ➧ ***DNS*** können Sie die Vorgehensweise bei der Namensauflösung auf **X4100/200/300** festlegen. In ***IP*** ➧ ***LOCAL SERVICES ACCESS CONTROL*** kann der Zugang zu den lokalen UDP- bzw. TCP-Diensten auf **X4100/200/300** geregelt werden.

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).
ISDN	In diesem Menü verwalten Sie das Taschengeldkonto (Credits Based Accounting System) von **X4100/200/300**.
CAPI	Enthält die Einstellungen für das ➤➤ **CAPI** User Concept von BinTec. Damit können Sie an Nutzer der CAPI-Anwendungen von **X4100/200/300** Benutzernamen und Paßwörter vergeben. So stellen Sie sicher, daß nur autorisierte Nutzer eingehende Rufe empfangen und ausgehende Verbindungen via CAPI aufbauen können.
QoS	In diesem Menü konfigurieren Sie alle Einstellungen zu "Quality of Service".
CONFIGURATION MANAGEMENT	In diesem Menü verwalten Sie die Konfigurationsdateien von **X4100/200/300**. Sie speichern Sie z. B. lokal auf **X4100/200/300** 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 **X4100/200/300**, 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 **X4100/200/300** wird diese Datei geladen. Mit ***EXIT*** ➧ **Exit without saving** verlassen Sie das Setup Tool, ohne die Konfiguration im Flash zu speichern.

Tabelle 4-5: Menüs im Setup Tool

4.5 Vorgehensweise für Initialkonfiguration

Wir empfehlen für die Initialkonfiguration von **X4100/200/300** folgende Vorgehensweise:

- Bereiten Sie die Konfiguration vor, wie in Kapitel 4.5.1, Seite 79 beschrieben.
- Installieren Sie die **BRICKware**, wie in Kapitel 4.5.2, Seite 80 beschrieben.
- Richten Sie Ihren PC ein, wie in Kapitel 4.5.3, Seite 81 beschrieben.
- Führen Sie die ersten Konfigurationsschritte über das MMI aus (siehe Kapitel 5, Seite 83). Dazu muß **X4100/200/300** noch nicht mit dem LAN verbunden sein, lediglich der Netzstecker muß angeschlossen sein:
  - gewünschte Display-Sprache einstellen
  - IP-Adresse und Netzmaske eintragen
- Schließen Sie **X4100/200/300** wie in Kapitel 3.4, Seite 46 beschrieben an.
- Erstellen Sie eine Grundkonfiguration mit Setup Tool (siehe Kapitel 6, Seite 101)
- Anschließend können Sie:
  - Weitere Funktionen mit dem Setup Tool konfigurieren (siehe Kapitel 7, Seite 179).
  - Ihre Erweiterungskarte mit dem Setup Tool konfigurieren (siehe Kapitel 8, Seite 287).
  - Sicherheitsfunktionen mit dem Setup Tool konfigurieren (siehe Kapitel 9, Seite 311).

4.5.1 Konfiguration vorbereiten

Bevor Sie die eigentliche Konfiguration von **X4100/200/300** vornehmen, müssen Sie einige Daten über Ihren ISDN-Anschluß und Ihre Netzwerkumgebung kennen.

Daten zurechtlegen

Tragen Sie in den folgenden Tabellen Ihre eigenen Werte ein, um diese bei der Konfiguration schnell zu finden. Beispiele sind angegeben:

Zugangsdaten	Beispielwert	Ihr Wert
ISDN-Rufnummern	*10*, *11*, *12*	
IP-Adresse von **X4100/ 200/300**	*192.168.1.254*	
Netzmaske von **X4100/ 200/300**	*255.255.255.0*	

- ISDN-Rufnummern: Die Rufnummern Ihres ISDN-Anschlusses.
- IP-Adresse und Netzmaske von **X4100/200/300**: Falls Sie ein neues Netzwerk einrichten, können Sie einfach die Beispielwerte übernehmen.

Internetzugang

Für den Internetzugang über Ihren Internet Service Provider (ISP), z. B. T-Online, benötigen Sie Zugangsdaten, die Sie von Ihrem ISP erhalten:

Zugangsdaten	Beispielwert	Ihr Wert
Providername	*GoInternet*	
Einwahlnummer	*1234567*	
Anschlußkennung	*MyName*	
Paßwort	*TopSecret*	

Firmennetzanbindung (LAN-LAN-Kopplung)

Für die Anbindung an eine Firmenzentrale oder einen anderen beliebigen WAN-Partner müssen Sie einige Daten der Gegenstelle kennen:

Zugangsdaten	Beispielwert	Ihr Wert
Partnername	*BigBoss*	

Zugangsdaten	Beispielwert	Ihr Wert
Einwahlnummer	***0911987654321***	
Lokaler Name	***LittleIndian***	
Paßwort	***Secret***	
Netzadresse(n) des Partners	***10.1.1.0***	
Netzmaske(n) des Partners	***255.255.255.0***	

Sprechen Sie die Daten mit Ihrem WAN-Partner ab: Sie beide verwenden das gleiche Paßwort; Ihr Eintrag "lokaler Name" und der Eintrag "Partnername" beim Partner müssen übereinstimmen; Ihr Eintrag "Partnername" und der Eintrag "lokaler Name" beim Partner müssen übereinstimmen.

TCP/IP-Protokoll prüfen und installieren

➤ Stellen Sie sicher, daß das TCP/IP-Protokoll auf dem PC installiert ist, bevor Sie mit der Konfiguration beginnen.

4.5.2 BRICKware installieren

BRICKware for Windows enthält Windows-Hilfsprogramme von BinTec Access Networks GmbH.

➤ Legen Sie Ihre BinTec Companion CD in das CD-ROM-Laufwerk Ihres PCs ein. Nach kurzer Zeit erscheint 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 auf **BRICKware**. Das Setup-Programm startet.

➤ Geben Sie das Verzeichnis an, in das **BRICKware** installiert werden soll.

Die **DIME Tools**, die Teil der **BRICKware for Windows** sind, umfassen hauptsächlich Hilfsprogramme zur Konfiguration, Wartung und Diagnose von **X4100/200/300**.

Eine detaillierte Beschreibung der Installation von **BRICKware** und die Beschreibung der einzelnen Komponenten finden Sie in **BRICKware for Windows** auf BinTecs WWW-Server.

4.5.3 PC einrichten

Mit X4100/200/300 ins Internet

Sie können über **X4100/200/300** einen WAN-Zugang, z. B. ins Internet, für alle PCs herstellen, die sich mit **X4100/200/300** in einem Netzwerk befinden. Dazu müssen Sie auf allen PCs, die bei der Konfiguration nicht als DHCP-Clients eingerichtet wurden, **X4100/200/300** als Gateway und als DNS-Server einrichten. Gehen Sie folgendermaßen vor:

- Zeigen Sie im Startmenü auf **Einstellungen** ➧ **Systemsteuerung**. Doppelklicken Sie auf **Netzwerk**.
- Wählen Sie **TCP/IP** in der Liste der Netzwerkkomponenten (unter Windows NT befindet sich diese im Register **Protokolle**) und klicken Sie auf **Eigenschaften**.
- Tragen Sie im Register **Gateway** unter **Neuer Gateway** die IP-Adresse von **X4100/200/300** ein. Klicken Sie auf **Hinzufügen**. (Windows NT: Tragen Sie im Register **IP-Adresse** unter **Standardgateway** die IP-Adresse von **X4100/200/300** ein.)
- Tragen Sie im Register **DNS-Konfiguration** unter **Suchreihenfolge für DNS-Server** die IP-Adresse des Gerätes **X4100/200/300** ein. Klicken Sie auf **Hinzufügen**, dann auf **OK**. Befolgen Sie die weiteren Anweisungen.

Windows 2000

- Klicken Sie im Windows-Startmenü auf **Einstellungen** ➧ **Netzwerk- und DFÜ-Verbindungen**.
- Doppelklicken Sie auf **LAN-Verbindung**.
- Klicken Sie im Register **Allgemein** auf **Eigenschaften**.
- Wählen Sie im Register **Allgemein** das **Internetprotokoll (TCP/IP)**. Klikken Sie auf **Eigenschaften**.
- Aktivieren Sie im Register **Allgemein** den Punkt **Folgende IP-Adresse verwenden**. Bestimmen Sie IP-Adresse, Netzmaske und Standard-Gateway. Als Standard-Gateway tragen Sie die IP-Adresse von **X4100/200/300** ein.
- Wenn Sie keinen eigenen DNS Server haben, geben Sie als DNS-Server-Adresse die IP-Adresse von **X4100/200/300** ein. Aktivieren Sie den Punkt **Folgende DNS-Serveradressen verwenden**.
- Geben Sie die IP-Adresse ein und klicken Sie auf **OK**.

- Schließen Sie die offenen Fenster mit **OK** bzw. **Schließen**.

Zum Schluß

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

5 Man Machine Interface (MMI) – Display mit Benutzerführung

BinTecs Man Machine Interface (MMI) mit Display und Eingabetasten erleichtert den "Ersten Kontakt" zu **X4100/200/300** und macht Statusinformationen leicht zugänglich.

Eine grafische Darstellung des MMI:

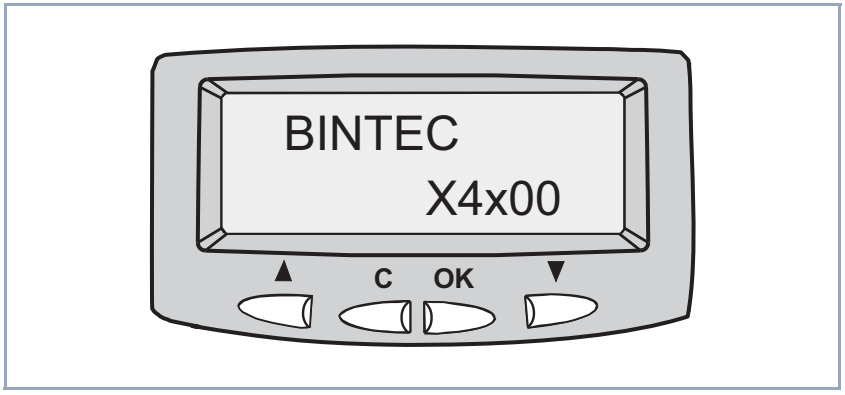


Bild 5-1: MMI mit Display und Eingabetasten und Geräte-Logo

Im diesem Kapitel finden Sie folgende Informationen:

- Einen Überblick über die Möglichkeiten des MMI (Kapitel 5.1, Seite 84)
- Eine Beschreibung, wie Sie das Display und die Eingabetasten benutzen (Kapitel 5.2, Seite 86)
- Eine Darstellung der Menüs des MMI und deren Einstellungen, hilfreich für die ersten Schritte (Kapitel 5.3, Seite 89)

Nachdem Sie die ersten Einstellungen mit dem MMI festgelegt haben, setzen Sie die Konfiguration von **X4100/200/300** mit dem Setup Tool (siehe Kapitel 6, Seite 101) fort.

5.1 Überblick

Erster Kontakt

Mit dem MMI können Sie IP-Adresse und Netzmaske von **X4100/200/300** eingeben, ohne vorher eine serielle Verbindung zu dem Gerät herstellen zu müssen. Dies erleichtert die Initialkonfiguration. So können Sie als erstes **X4100/200/300** eine IP-Adresse zuweisen und dann das Gerät an dem dafür vorgesehenen Standort aufstellen und anschließen. Die Konfiguration erfolgt dann von Ihrem Rechner aus über Ihr Netzwerk (z. B. per Setup Tool).

Statusinformationen

Durch die Anzeige von Statusinformationen im MMI wird das Monitoring der Aktivitäten von **X4100/200/300** ermöglicht, ohne sich einloggen zu müssen. Damit wird ein zusätzliches Diagnose-Tool bereitgestellt, das z. B. den aktuelle Stand der System-Software oder die Aktivitäten der Geräte-Schnittstellen anzeigt.

Benutzerführung

Beleuchtete Eingabetasten und Navigationsleisten erleichtern die Bedienung des MMI. Sie werden so durch die Menüstruktur geführt, daß Sie Einstellungen in jedem Menü vornehmen können, ohne jedes Menü einzeln suchen zu müssen. Trotzdem können Sie auch gezielt ein ganz bestimmtes Menü aufsuchen.

Logo

Nach dem Anschalten führt **X4100/200/300** zunächst einige Selbsttests durch und zeigt anschließend das Geräte-Logo auf dem Display an (siehe Bild 5-1, Seite 83). Betätigen Sie eine beliebige Eingabetaste, um das MMI zu benutzen. Wenn über längere Zeit keine Eingaben mehr gemacht werden, wechselt das MMI wieder zum Logo. Der Zeitraum kann im Menü "Display-Idletimer" eingestellt werden.

Die Voreinstellung zeigt beim Einschalten von **X4100/200/300** bzw. nach dem Ablauf des Display-Idletimers das Geräte-Logo an.

Sie können das Geräte-Logo durch jedes beliebige MMI-Menü ersetzen, indem Sie das gewünschte Menü auf dem Display anzeigen und dann gleichzeitig **C** und **OK** drücken. Nach Ablauf des Idletimers erscheint dann das entsprechende Menü anstelle des Logos. Auf diese Weise könnten Sie z. B. eine bestimmte Schnittstelle von **X4100/200/300** anzeigen und überwachen.

Zugriffsschutz

Die Voreinstellung betreibt das MMI im Konfigurationsmodus, in dem alle Funktionen des MMI genutzt werden können. Im Monitoring-Modus dagegen kann jedes Menü angezeigt werden, Eingaben sind aber nur begrenzt möglich. So kann im Monitoring-Modus z. B. die eingetragene IP-Adresse angezeigt, aber nicht verändert werden.

Das Umstellen vom Monitoring-Modus in den Konfigurationsmodus und umgekehrt nehmen Sie im Hauptmenü "Display-Einstellungen" vor, siehe Kapitel 5.3.1, Seite 90.

5.2 Display und Eingabetasten

Im folgenden wird erläutert, wie Sie mit dem Display und den Eingabetasten des MMI umgehen können.

5.2.1 Eingabetasten verwenden

Um den Umgang mit den Eingabetasten zu verdeutlichen, zeigt Bild 5-2, Seite 86 einen Ausschnitt des Menüsystems:

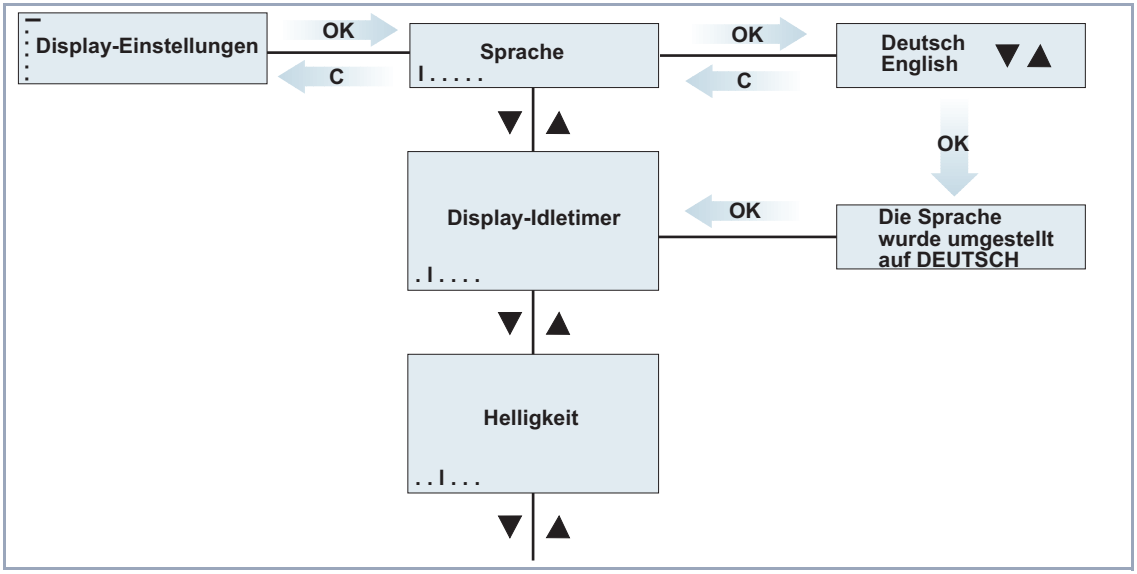


Bild 5-2: Verwenden der Eingabetasten (Ausschnitt aus Menüsystem)

Navigieren mit ▼ und ▲

Mit den Pfeiltasten bewegen Sie sich innerhalb des Menüsystems nach unten bzw. nach oben. Sie bewegen sich immer nur auf einer Ebene, wechseln z. B. von einem Hauptmenü zum anderen.

Menü auswählen mit OK

Um einen Menüpunkt auszuwählen, bestätigen Sie mit **OK**. Damit wechseln Sie auf die darunterliegende Ebene, innerhalb der Sie sich auch wieder mit Hilfe von ▼ und ▲ bewegen können.

Im Menü

In einem Menü können Sie folgende Aktionen ausführen:

- Einen Wert (z. B. Helligkeit des Displays) mit ▼ und ▲ auswählen und anschließend mit **OK** bestätigen.
- Ziffern (z. B. IP-Adresse oder PIN) mit ▼ und ▲ eingeben und anschließend mit **OK** bestätigen.
- Einen Wert (z. B. Seriennummer von **X4100/200/300**) anzeigen und anschließend das Menü mit **OK** verlassen.

Menü mit C verlassen

Um ein Menü zu verlassen und in das darüberliegende zu wechseln, ohne eine Einstellung zu verändern, drücken Sie einfach **C**.

5.2.2 Bedeutung der LEDs

Benutzerführung

Die vier Eingabetasten des MMI sind mit LEDs hinterlegt (siehe Tabelle 5-1, Seite 87) und gestatten Ihnen so eine einfache und komfortable Bedienung. Nur die Tasten sind beleuchtet, die zum jeweiligen Zeitpunkt benutzt werden können. Das Drücken der nicht-beleuchteten Tasten hat keine Auswirkung:

Taste	LED an	LED aus
C	Durch Drücken ist das Verlassen der Menüebene möglich	Keine sinnvolle Eingabe möglich
▲	Durch Drücken ist Rückwärtsbewegung in der Menüebene möglich	Keine sinnvolle Eingabe möglich
▼	Durch Drücken ist Vorwärtsbewegung in der Menüebene möglich	Keine sinnvolle Eingabe möglich
OK	Eingabe oder Auswahl bestätigen ist möglich	Keine sinnvolle Eingabe möglich

Tabelle 5-1: Beleuchtung der Eingabetasten

5.2.3 Navigationsleisten und Menüstruktur

Navigationsleisten zur Orientierung

Auf dem Display sind zwei Navigationsleisten abgebildet, die anzeigen, auf welcher Ebene im Menüsystem Sie sich gerade befinden:

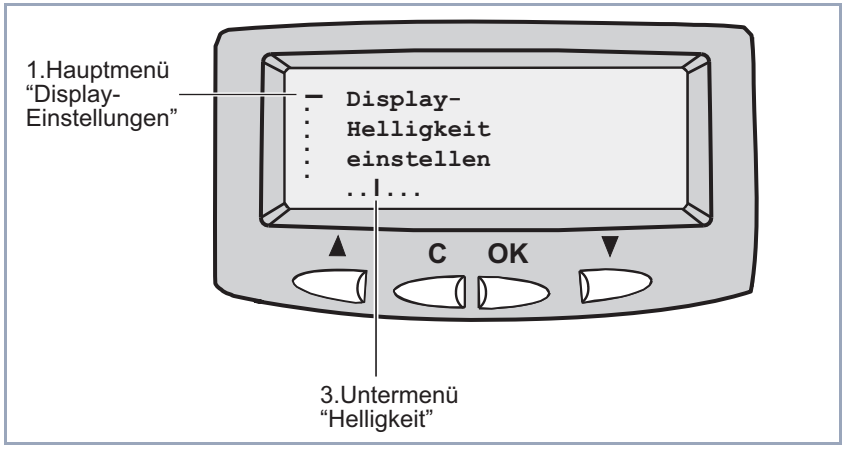


Bild 5-3: Navigationsleisten (Beispiel)

Die vertikale Navigationsleiste am linken Rand des Displays bezieht sich auf die Hauptmenüs. Die horizontale Navigationsleiste am unteren Rand zeigt an, in welchem Menü der zweiten Ebene innerhalb des entsprechenden Hauptmenüs Sie sich befinden.

Die folgenden Abbildungen zeigen die Menüstrukturen mit den dazugehörigen Navigationsleisten.

5.3 Menüs und Einstellungen

Das MMI bietet folgende Menüs auf der obersten Ebene (Hauptmenüs):

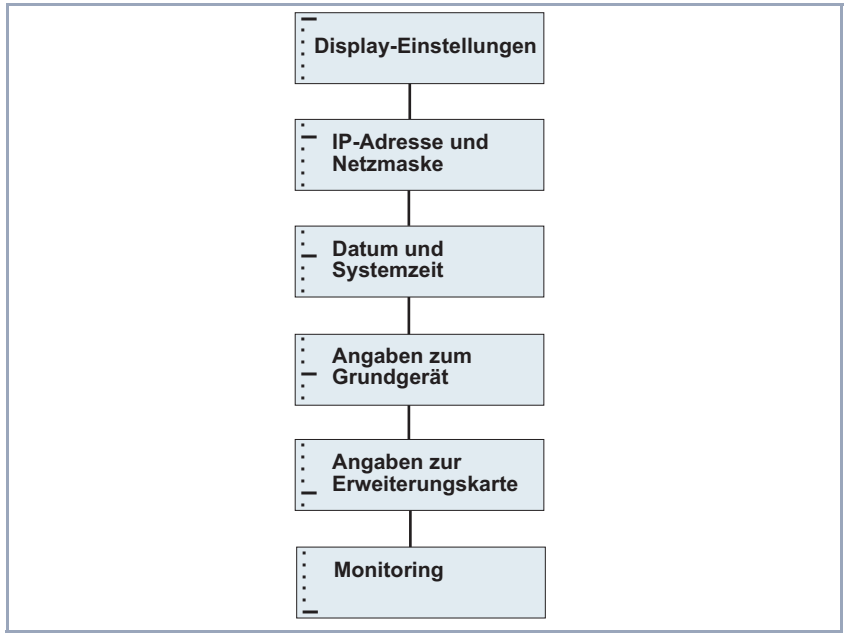


Bild 5-4: Hauptmenüs (mit Navigationsleisten)

- **Display-Einstellungen** (siehe Kapitel 5.3.1, Seite 90)
- **IP-Adresse und Netzmaske** (siehe Kapitel 5.3.2, Seite 92)
- **Datum und Systemzeit** (siehe Kapitel 5.3.3, Seite 93)
- **Angaben zum Grundgerät** (siehe Kapitel 5.3.4, Seite 94)
- **Angaben zur Erweiterungskarte** (siehe Kapitel 5.3.5, Seite 95)
- **Monitoring** (siehe Kapitel 5.3.6, Seite 96)

Die folgenden Abbildungen zeigen die Struktur der einzelnen Menüs. Diese zu durchlaufen, stellt eine gute Möglichkeit dar, die ersten Schritte mit dem MMI auszuführen.

5.3.1 Display-Einstellungen

Hier eine grafische Darstellungen der Menüs für Display-Einstellungen:

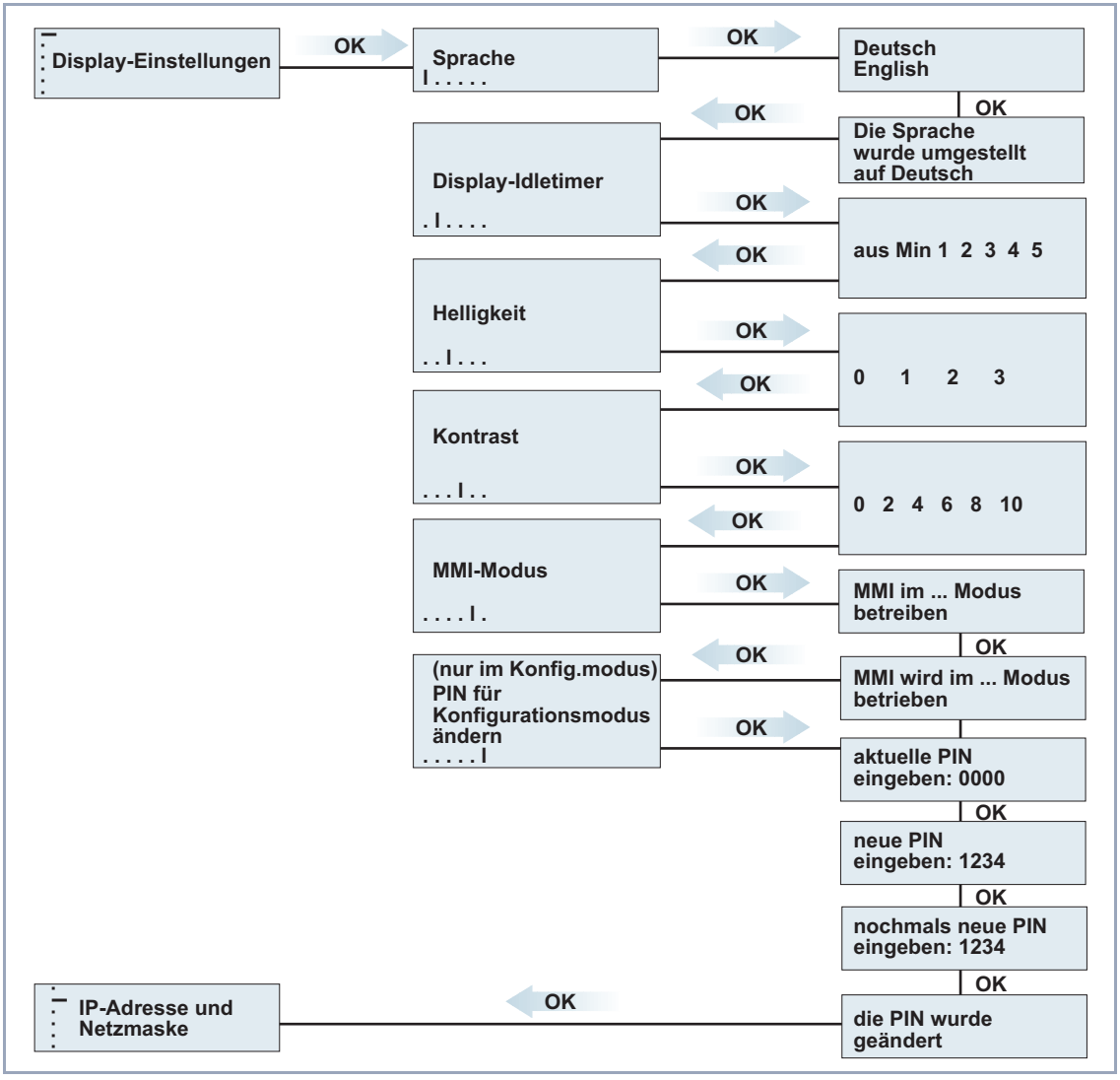


Bild 5-5: Menüs zum Auswählen der Display-Einstellungen (mit Navigationsleisten)

Das Hauptmenü "Display-Einstellungen" bietet folgende Möglichkeiten zur Anpassung der Display-Eigenschaften:

- **Sprache**
  Hier stellen Sie die Sprache des Displays ein. Standardmäßig ist zunächst Englisch voreingestellt.

- **Display-Idletimer**
  Hier aktivieren bzw. deaktivieren Sie den Display-Idletimer ein (1 bis 5 Minuten). Nach Ablauf dieser Zeit erscheint das Logo auf dem Display, wenn so lange keine Eingabetaste benutzt wurde.

- **Helligkeit**
  Hier stellen Sie die Helligkeit des Displays ein.

- **Kontrast**
  Hier stellen Sie den Kontrast des Displays ein.

- **MMI-Modus**
  Hier können Sie vom Konfigurationsmodus in den Monitoring-Modus wechseln und umgekehrt. Um in den Konfigurationsmodus zu wechseln, benötigen Sie die eingestellte PIN.

- **PIN für Konfigurationsmodus ändern**
  Hier können Sie die PIN (Persönliche Identifikations-Nummer) für den Konfigurationsmodus ändern.
  Der Konfigurationsmodus ist durch eine vierstellige PIN geschützt. Die Voreinstellung der PIN im Auslieferungszustand lautet **0000**. Beim ersten Benutzen des MMI sollten Sie die PIN ändern, um Eingaben von unberechtigten Benutzern zu verhindern. Aus technischen Gründen wird die PIN auf dem Display im Klartext angezeigt. Achten Sie bei der Eingabe der PIN also darauf, daß das Display gegen Fremdeinsicht geschützt ist.
  Benutzer, denen die eingestellte PIN nicht bekannt ist, können nicht vom Monitoring-Modus in den Konfigurationsmodus wechseln.

5.3.2 IP-Adresse und Netzmaske

Das Hauptmenü "IP-Adresse und Netzmaske" bietet folgende Möglichkeiten:

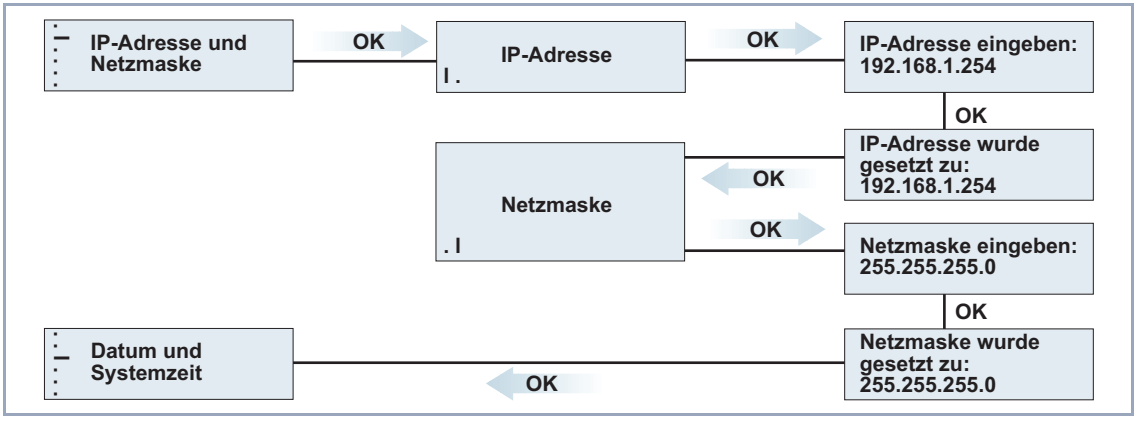


Bild 5-6: Menüs zum Eingeben von IP-Adresse und Netzmaske (mit Navigationsleisten)

- **IP-Adresse**
  Hier geben Sie die IP-Adresse von **X4100/200/300** ein. Dazu wählen Sie jede Ziffer mit ▼ und ▲ aus und bestätigen jeweils mit **OK**. Nach Bestätigen der letzten Ziffer ist die IP-Adresse gespeichert.

- **Netzmaske**
  Hier geben Sie die Netzmaske des Netzwerks ein, in dem sich das Gerät befindet. Dazu betätigen Sie so oft ▼ und ▲, bis die korrekte Netzmaske erscheint. Nach Bestätigen mit **OK** ist die Netzmaske gespeichert.

5.3.3 Datum und Systemzeit

Das Hauptmenü "Datum und Systemzeit" bietet folgende Möglichkeiten:

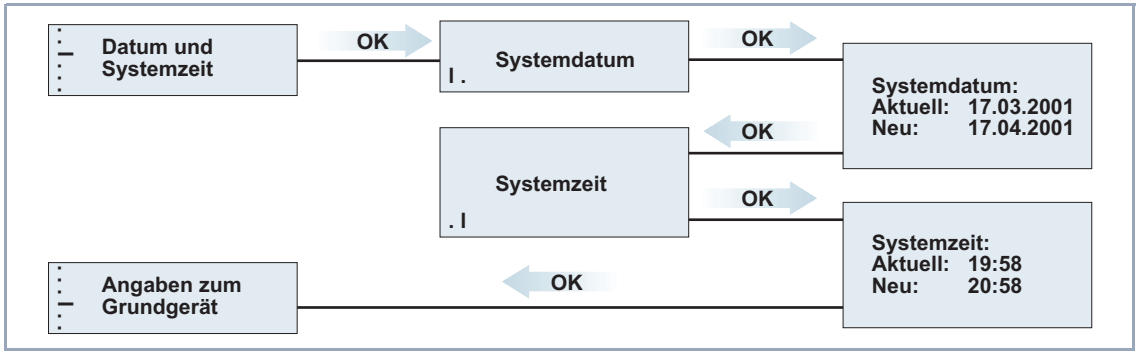


Bild 5-7: Menüs zum Eingeben von Datum und Systemzeit (mit Navigationsleisten)

- **Systemdatum**
  Hier stellen Sie das aktuelle Datum auf **X4100/200/300** ein. Dazu wählen Sie mit ▼ und ▲ nacheinander Tag, Monat und Jahr aus und bestätigen jeweils mit **OK**.

- **Systemzeit**
  Hier stellen Sie die aktuelle Uhrzeit auf **X4100/200/300** ein. Dazu wählen Sie mit ▼ und ▲ nacheinander Stunden und Minuten aus und bestätigen jeweils mit **OK**.

5.3.4 Angaben zum Grundgerät

Das Hauptmenü "Angaben zum Grundgerät" bietet folgende Möglichkeiten zur Anzeige von Systeminformationen:

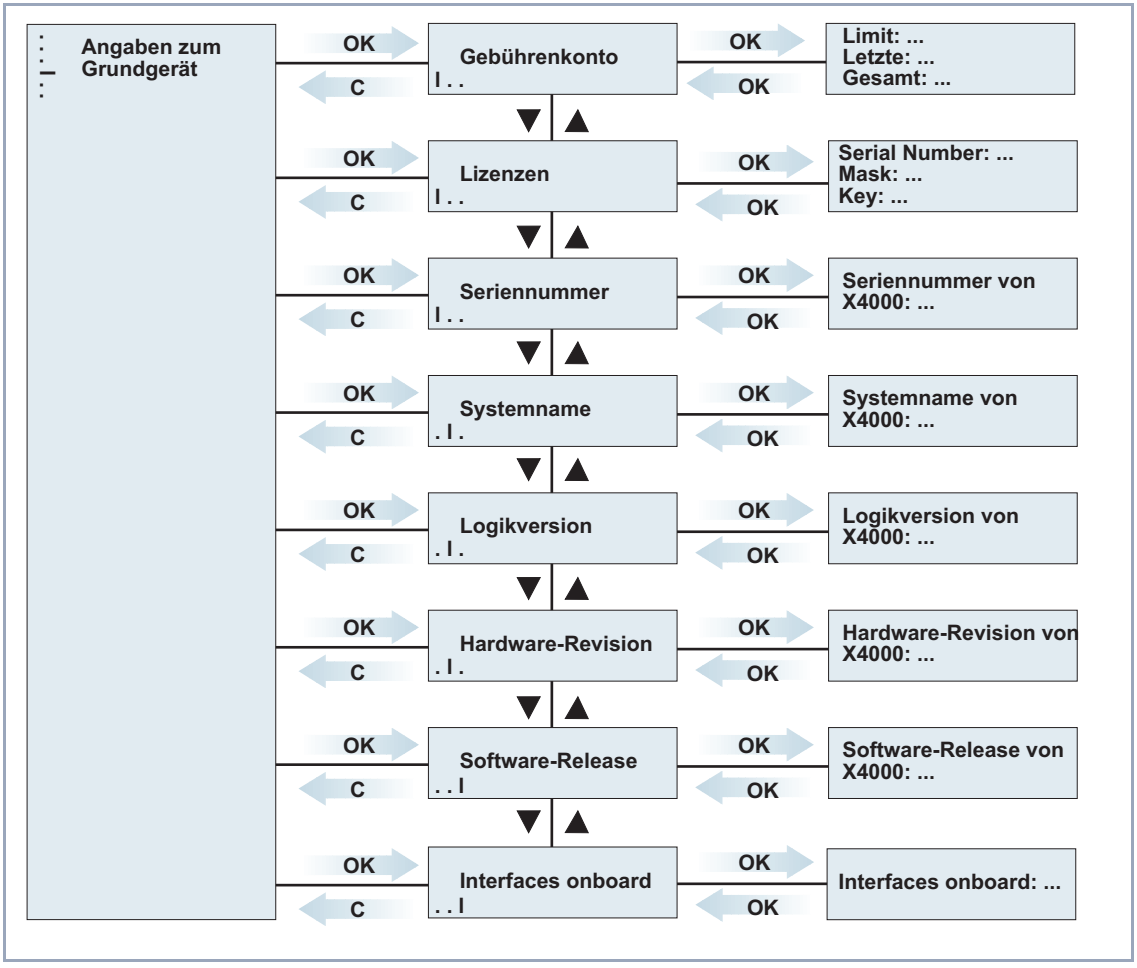


Bild 5-8: Menüs zum Monitoring des Grundgeräts (mit Navigationsleisten)

- **Gebührenkonto**
  Hier werden die Einstellungen für das Taschengeldkonto (Credits Based Accounting System, siehe Kapitel 9.1.3, Seite 321) angezeigt.
  Limit: Eingestelltes Gebührenlimit.
  Letzte: Kosten der letzten Verbindung.
  Gesamt: Bisher angefallene Kosten.

- **Lizenzen**
  Hier werden die auf **X4100/200/300** eingetragenen Lizenzen angezeigt (siehe Kapitel 6.1.1, Seite 102).

- **Seriennummer**
  Hier wird die Seriennummer von **X4100/200/300** angezeigt.

- **Systemname**
  Hier wird der Systemname von **X4100/200/300** angezeigt (siehe Kapitel 6.1.2, Seite 106).

- **Logikversion**
  Hier wird die Version der Firmware-Logik von **X4100/200/300** angezeigt.

- **Hardware-Revision**
  Hier wird die Hardware-Revision von **X4100/200/300** angezeigt.

- **Software-Release**
  Hier wird die Version der System-Software von **X4100/200/300** angezeigt.

- **Interfaces onboard**
  Hier wird der Status der Hardware-Schnittstellen von **X4100/200/300** angezeigt, die mit dem Grundgerät verfügbar sind.

5.3.5 Angaben zur Erweiterungskarte

Angaben zu den Schnittstellen auf der optionalen Erweiterungskarte können erst angezeigt werden, wenn die entsprechende Karte eingebaut ist. Bitte beachten Sie nachfolgende Software-Releases und die entsprechenden **Release Notes**.

5.3.6 Monitoring

Das Hauptmenü "Monitoring" bietet die Möglichkeit zur Überwachung der Betriebstemperatur von **X4100/200/300**-Geräten:

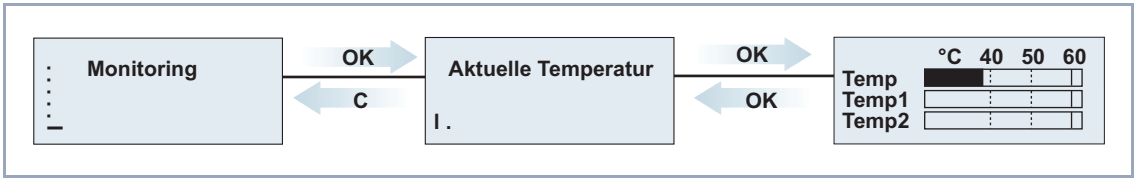


Bild 5-9: Menüs zum Monitoring von **X4100/200/300**

Aktuelle Temperatur

Hier wird die aktuelle Betriebstemperatur von **X4100/200/300** in Celsius angezeigt.

Die aktuelle Betriebstemperatur wird jeweils mit einem schwarzen Balken angezeigt. **Temp** zeigt die Temperatur an, die von einem Sensor im Grundgerät gemessen wird, **Temp1** und **Temp2** zeigt die auf der Erweiterungskarte gemessene Temperatur an. Eine PRI-Erweiterungskarte verfügt über zwei Temperatursensoren, eine BRI- und eine LAN-Erweiterungskarte verfügen über jeweils einen Sensor (**Temp1**).

Der Wert für die maximal zulässige Temperatur liegt derzeit bei 60 °C und wird jeweils mit einer durchgezogenen Linie auf dem Display angezeigt. Die maximal zulässige Temperatur kann durch Editieren folgender MIB-Variablen verändert werden:

- für das Grundgerät (**Temp**):
  sysX4ConfigTempAlarmTrap
- für die Erweiterungskarten (**Temp1** und **Temp2**):
  sysX4ConfigTempAlarmTrapMod
  sysX4ConfigTempAlarmTrapMod2

Bei Überschreiten dieser Temperatur erzeugt **X4100/200/300** Traps, die über das Netzwerk ausgewertet werden können.

5.3.7 Default-Screen festlegen

In der Voreinstellung wird nach Ablauf des Idletimers das Logo auf dem Display angezeigt. Um ein anderes Menü des MMI als Default-Screen zu verwenden, gehen Sie folgendermaßen vor:

➤ Zeigen Sie unter Verwendung der Eingabetasten das gewünschte Menü an.

➤ Halten Sie die Taste **C** für die Dauer von drei Sekunden gedrückt.

Das MMI zeigt folgenden Text:

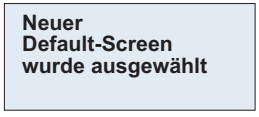


Bild 5-10: Neues Menü als Default-Screen ausgewählt

➤ Bestätigen Sie mit **OK**.

Das ausgewählte Menü wird angezeigt und als Default-Screen verwendet.

5.3.8 Konfiguration sichern

Gehen Sie folgendermaßen vor, um die aktuelle Konfiguration von **X4100/200/300** durch die Verwendung der Eingabetasten zu sichern:

➤ Halten Sie die Taste **OK** für die Dauer von drei Sekunden gedrückt.

Das MMI zeigt folgenden Text:

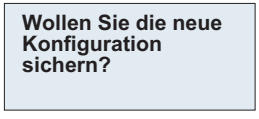


Bild 5-11: Konfiguration sichern über MMI

➤ Drücken Sie **OK**.

Das MMI zeigt nacheinander folgenden Text:

Bild 5-12: Status der Konfigurationssicherung

➤ Drücken Sie **OK**.

Die Konfiguration ist im Flash gespeichert.

5.3.9 X4100/200/300 neustarten

Gehen Sie folgendermaßen vor, um **X4100/200/300** durch Verwendung der Eingabetasten neu zu starten:

➤ Halten Sie die Tasten **OK** und **C** für die Dauer von drei Sekunden gedrückt.

Das MMI zeigt folgenden Text:

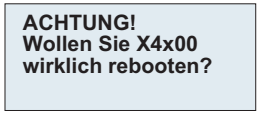


Bild 5-13: **X4100/200/300** neustarten über MMI

➤ Drücken Sie **OK**.

Das MMI zeigt folgenden Text:

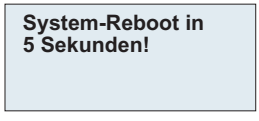


Bild 5-14: Ankündigung Neustart

Nach fünf Sekunden wird der Neustart ausgeführt.

Das MMI zeigt folgenden Text:

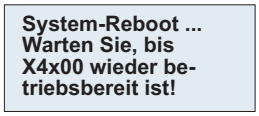


Bild 5-15: Neustart **X4100/200/300**

Nach dem Neustart von **X4100/200/300** wird nach Ablauf der Default-Zeit der Default-Screen des MMI dargestellt.

6 Basiskonfiguration des Grundgeräts mit dem Setup Tool

In diesem Kapitel erfahren Sie, wie Sie die grundlegenden Konfigurationsschritte für die Inbetriebnahme Ihres **X4100/200/300**-Grundgerätes mit dem Setup Tools durchführen.

Das Kapitel ist folgendermaßen aufgebaut:

- Vorbereitende Routereinstellungen (Kapitel 6.1, Seite 102)
  Hier sind die Schritte beschrieben, die Sie für den Betrieb von **X4100/200/300** in jedem Fall durchführen müssen, unabhängig davon, in welcher Umgebung bzw. für welche Applikationen Sie **X4100/200/300** nutzen.
  - Wie geht's jetzt weiter? (Kapitel 6.1.6, Seite 119)
    Nachdem Sie die grundlegenden Routereinstellungen vorgenommen haben, können Sie sich mit Hilfe dieses Kapitels orientieren, wie Sie fortfahren können.
- WAN-Schnittstellen konfigurieren (Kapitel 6.2, Seite 121)
  Beschreibung, wie Sie die im **X4100/200/300**-Grundgerät integrierten WAN-Schnittstellen konfigurieren.
- WAN-Partner konfigurieren (Kapitel 6.3, Seite 147)
  Beschreibung, wie Sie Ihre WAN-Partner einrichten.
- Konfiguration sichern (Kapitel 6.4, Seite 176)
  So sichern Sie Ihre Konfiguration.
- Kommunikationsanwendungen für CAPI auf Ihrem PC konfigurieren (Kapitel 6.5, Seite 177)
- Konfiguration testen (Kapitel 6.6, Seite 178)
  So testen Sie Ihre Konfiguration.

6.1 Vorbereitende Routereinstellungen

Vorbereitende Routereinstellungen betreffen **X4100/200/300** und Ihr lokales Netzwerk:

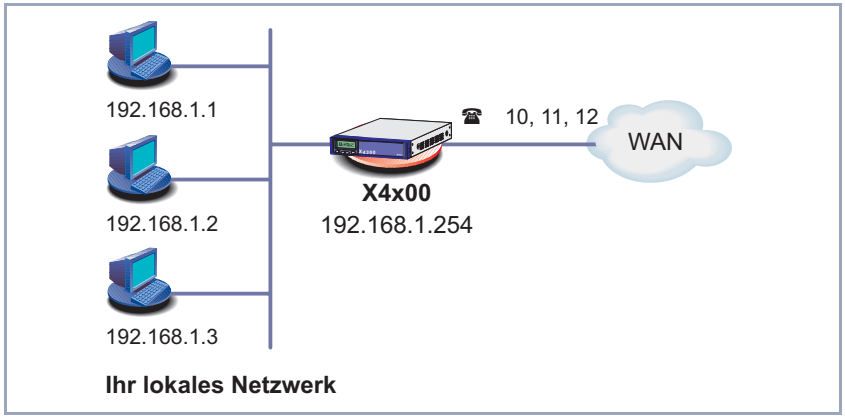


Bild 6-1: Grundlegende Routereinstellungen – **X4100/200/300** im LAN

Folgende Schritte sind erforderlich:

- Gegebenenfalls Lizenz eintragen (Kapitel 6.1.1, Seite 102)
- Systemdaten (z. B. Paßwörter) eintragen (Kapitel 6.1.2, Seite 106)
- LAN-Schnittstelle konfigurieren (Kapitel 6.1.3, Seite 108)
- Gerät der **X4100/200/300** als DHCP-Server einrichten (optional) (Kapitel 6.1.4, Seite 112)
- NetBIOS-Filter setzen (optional) (Kapitel 6.1.5, Seite 115)

Wie Sie die PCs in Ihrem Netzwerk einrichten, finden Sie in Kapitel 4.5.3, Seite 81 beschrieben.

6.1.1 Lizenz(en)

Zusatzlizenz In diesem Kapitel wird beschrieben, wie Sie die Funktionen Ihrer gegebenenfalls erworbenen Software- bzw. Hardware-Lizenz freischalten.

Lizenzdaten

Die Lizenzdaten umfassen die Hardware-Seriennummer Ihres Gerätes bzw. Ihrer Erweiterungskarte, eine PIN und eine Lizenzseriennummer. Die beiden letzteren Daten erhielten Sie mit Ihrer Zusatzlizenz. Bei der Online-Lizenzierung geben Sie die oben genannten Lizenzdaten ein und erhalten einen Key. Diesen Key geben Sie zusammen mit Ihrer Lizenzseriennummer (Serial Number) im Setup Tool ein, um die Funktionen Ihrer Zusatzlizenz auf **X4100/200/300** freizuschalten.

Lizenz eintragen

Gehen Sie folgendermaßen vor, um eine Lizenz einzutragen:

- Loggen Sie sich mit dem Benutzernamen `admin` auf **X4100/200/300** ein, wie in Kapitel 4.2, Seite 62 beschrieben.
- Rufen Sie das Setup Tool mit `setup` auf.
- Gehen Sie zu ***LICENSES***.

Unter **Available Licenses** sind die auf **X4100/200/300** verfügbaren Subsysteme aufgelistet:

```
X4x00 Setup Tool                              BinTec Access Networks GmbH
[LICENSE]: Licenses                                              MyRouter

Available Licenses:

IP (builtin), STAC, CAPI, BRIDGE


Serialnumber     Mask     Key             Description      State
101546           55       88PNUPZ         composite        ok


ADD                       DELETE                        EXIT

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

Außerdem zeigt das Menü die eingetragenen Lizenzen (**Serialnumber**, **Mask**, **Key**).

Auslieferungszustand

Folgende Lizenzen stehen auf **X4100/200/300** im Auslieferungszustand zur Verfügung:

Lizenzen im Auslieferungszustand	Bedeutung
IP	IP-Routing
STAC	➤➤ **STAC-**➤➤ **Datenkompression**
CAPI	➤➤ **Remote-CAPI**-Schnittstelle, ermöglicht Kommunikationsanwendungen auf Ihrem Rechner, z. B. Faxe versenden und empfangen
BRIDGE	Bridging

Tabelle 6-1: Lizenzierte Subsysteme im Auslieferungszustand

Ab Mai 2003 ist die STAC-Lizenz nicht mehr im Auslieferungszustand enthalten. Sie erhalten jedoch eine kostenlose Lizenz unter www.bintec.de.

Subsysteme mit Lizenz erhältlich

Folgende Subsysteme stehen nach entsprechender Lizenzierung auf **X4100/200/300** zur Verfügung:

Subsysteme	Bedeutung
X25	X.25
OSPF	Open Shortest Path First
TAF	Token Authentication Firewall
TUNNEL	Virtual Private Networking (VPN, PPTP)
FRAME RELAY	Frame Relay
IPSec	Internet Protocol Security

Tabelle 6-2: Subsysteme mit Zusatzlizenz

ToDo Gehen Sie folgendermaßen vor, um eine Lizenz einzutragen:

- Fügen Sie einen neuen Eintrag mit **ADD** hinzu.

  Ein weiteres Menüfenster öffnet sich.

- Geben Sie **Serial Number** (die Lizenzseriennummer, die Sie beim Kauf der Lizenz erhalten haben) und **Key** (bei der Online-Lizenzierung erhalten) ein.

- Bestätigen Sie mit **SAVE.**

  Sie befinden sich wieder im Menü ***LICENSES***. Die mit Ihrer Lizenz freigeschalteten Subsysteme sind aufgelistet. Die eingetragene Lizenz wird mit dem Status *ok* angezeigt.

Wenn als Status *not ok* angezeigt wird:

- Geben Sie die Lizenzdaten erneut ein.

Wird der Status *not_supported* angezeigt, dann haben Sie eine Lizenz für ein Subsystem eingegeben, das ihr Router nicht unterstützt. Sie werden die Funktionen dieser Lizenz also nicht nutzen können.

Lizenz ausschalten Gehen Sie folgendermaßen vor, um eine Lizenz auszuschalten:

- Gehen Sie zu ***LICENSES***.
- Markieren Sie die gewünschte Lizenz.
- Bestätigen Sie mit **DELETE**.

  Die Lizenz ist ausgeschaltet. Sie können Ihre Zusatzlizenz jederzeit durch Eingabe des gültigen **Key**s und der **Serial Number** (Lizenzseriennummer) wieder aktivieren.

Es kommt vor, daß die Lizenzen des Auslieferungszustandes gelöscht werden. Gehen Sie folgendermaßen vor, um die gelöschten Lizenzen wieder zu aktivieren:

- Gehen Sie zu ***LICENSES*** ➧ **ADD**.
- Tragen Sie die **Mask** *65535* ein.
- Belassen Sie alle anderen Felder leer.
- Bestätigen Sie mit der **Eingabetaste**.

  Die Lizenzen des Auslieferungszustandes sind wieder aktiviert.

6.1.2 Systemdaten eintragen

Tragen Sie als nächstes die grundlegenden Systemdaten von **X4100/200/300** ein.

➤ Gehen Sie zu ***SYSTEM***.

Folgendes Menü öffnet sich:

```
X4x00 Setup Tool                          BinTec Access Networks GmbH
[SYSTEM]: Change System Parameters                          MyRouter

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

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

External Activity Monitor>
External System Logging>
Keepalive Monitoring>
Password settings>
Time and Date>

            SAVE                                CANCEL

Enter string, max length = 34 chars
```

Folgende Felder des Menüs sind für diesen Konfigurationsschritt relevant:

Feld	Bedeutung
System Name	Definiert den Systemnamen von **X4100/200/300**, wird auch als PPP-Host-Name benutzt. Erscheint beim Einloggen auf dem Gerät 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 **X4100/200/300** nötig, wenn eine nicht-partnerspezifische ➤➤ **PPP-Authentisierung** (z. B. ➤➤ **PAP** oder ➤➤ **CHAP**) durchgeführt wird (siehe Kapitel 7.1.3, Seite 186).

Feld	Bedeutung
Location	(optional) Gibt an, wo sich **X4100/200/300** befindet.
Contact	(optional) Gibt die zuständige Kontaktperson an. Hier kann z. B. die E-Mail-Adresse des Systemadministrators eingetragen werden.

Tabelle 6-3: ***System***

Paßwörter

Im Untermenü ***System*** ➧ ***Password settings*** geben Sie die Paßwörter für **X4100/200/300** ein:

Feld	Bedeutung
admin Login Password	Paßwort für Benutzername `admin`.
read Login Password	Paßwort für Benutzername `read`.
write Login Password	Paßwort für Benutzername `write`.

Tabelle 6-4: ***System*** ➧ ***Password settings***

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. Die Vorgehensweise bei der Änderung von Paßwörtern ist unter Kapitel 4.4.4, Seite 71 beschrieben.

➤ Ändern Sie unbedingt die Paßwörter, um unberechtigten Zugriff auf **X4100/200/300** zu verhindern.

Die Befugnisse der Benutzernamen und Paßwörter finden Sie in Kapitel 4.2, Seite 62.

ToDo

Gehen Sie folgendermaßen vor, um die relevanten Systemdaten und Paßwörter einzutragen:

➤ Geben Sie **System Name** von **X4100/200/300** ein, z. B. ***MyRouter***.

➤ 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***.
- Gehen Sie zu ***System*** ➧ ***Password settings***.
- Geben Sie **admin Login Password** ein.
- Geben Sie **read Login Password** ein.
- Geben Sie **write Login Password** ein.
- Bestätigen Sie mit **SAVE**.

  Sie befinden sich im Menü ***SYSTEM***.
- Bestätigen Sie mit **SAVE**.

  Sie befinden sich wieder im Hauptmenü. Die Eintragungen sind temporär gespeichert und aktiviert.

Weiterführende Konfiguration

Im Menü ***System*** ➧ ***External Activity Monitor*** finden Sie die Einstellungen, die nötig sind, um **X4100/200/300** mit dem Windows-Tool Activity Monitor überwachen zu können (siehe Kapitel 9.1.4, Seite 325 bzw. **BRICKware for Windows**).

Im Menü ***System*** ➧ ***External System Logging*** finden Sie Einstellungen für Syslog-Messages (siehe Kapitel 9.1.1, Seite 312).

Im Menü ***System*** ➧ ***Keepalive Monitoring*** finden Sie Einstellungen für die Funktion "Keepalive Monitoring" (siehe Kapitel 7.2.12, Seite 227).

Im Menü ***System*** ➧ ***Time and Date*** finden Sie Einstellungen zur manuellen Eingabe von Uhrzeit und Datum auf **X4100/200/300** (siehe Kapitel 7.3.1, Seite 233).

6.1.3 LAN-Schnittstelle konfigurieren

Dieses Kapitel beschreibt die Konfiguration der LAN-Schnittstelle (10/100 Base-T Ethernet) von **X4100/200/300**. Die LAN-Schnittstelle ist die physikalische Schnittstelle zum lokalen Netzwerk. Im Menü ***CM-100BT, Fast Ethernet*** geben Sie Ihrem Router die Adresse, unter der er im LAN zu erreichen ist. So-

lange auf Ihrem Router diese Werte nicht eingetragen sind, kann er von anderen Hosts im Netzwerk nicht erkannt werden.

In diesem Kapitel wird nur die Konfiguration von ➤➤ **IP** erläutert. Belassen Sie die unter **Bridging** voreingestellten Werte.

Beispiel Teilnetze

Falls Ihr **X4100/200/300** an ein LAN angeschlossen ist, das aus zwei Teilnetzen besteht, sollten Sie für das zweite Teilnetz eine **Second Local IP Number** und eine **Second Local Netmask** eintragen.

Beispiel eines LANs mit Teilnetzen:

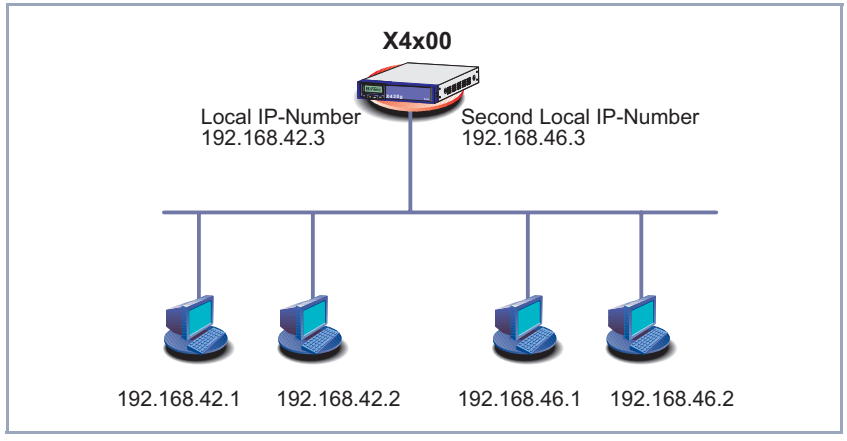


Bild 6-2: Gerät der **X4100/200/300** mit zwei verschiedenen lokalen IP-Adressen

Im ersten Teilnetz gibt es zwei Hosts mit den IP-Adressen 192.168.42.1 und 192.168.42.2, im zweiten Teilnetz zwei Hosts mit den IP-Adressen 192.168.46.1 und 192.168.46.2. Um mit dem ersten Teilnetz Datenpakete austauschen zu können, benutzt **X4100/200/300** z. B. die IP-Adresse 192.168.42.3, für das zweite Teilnetz 192.168.46.3. Die Netzmasken für beide Teilnetze müssen ebenfalls angegeben werden.

Vermutlich haben Sie auf **X4100/200/300** schon vor der Grundkonfiguration IP-Adresse und Netzmaske über das MMI eingetragen. Überprüfen Sie trotzdem die Eintragungen im Menü ***CM-100BT, FAST ETHERNET.***

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

Gehen Sie folgendermaßen vor:

➤ Gehen Sie zu ***CM-100BT, FAST ETHERNET***.

Folgendes Menü öffnet sich:

```
X4x00 Setup Tool                          BinTec Access Networks GmbH
[LAN]: Configure LAN Interface                                MyRouter

IP-Configuration
    local IP-Number          192.168.1.254
    local Netmask            255.255.255.0
    Second Local IP-Number
    Second Local Netmask
    Encapsulation            Ethernet II
    Mode                     Auto

Bridging                disabled

Advanced Settings>

            SAVE                          CANCEL

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

In diesem Menü sind Einträge für IP-Konfiguration und ➤➤ **Bridging** möglich.

Folgende Felder des Menüs sind für die Konfiguration der LAN-Schnittstelle relevant:

Feld	Bedeutung
local IP-Number	IP-Adresse von **X4100/200/300** im LAN.
local Netmask	Netzmaske des Netzwerkes, in dem sich **X4100/200/300** mit **local IP-Number** befindet.
Second Local IP-Number	Zweite IP-Adresse von **X4100/200/300** im LAN.
Second Local Netmask	Netzmaske des Netzwerkes, in dem sich **X4100/200/300** mit **Second Local IP-Number** befindet.

Feld	Bedeutung
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* Sie können i. a. den Standardwert *Ethernet II* belassen. Mit *Ethernet II* heißt die LAN-Schnittstelle en1, mit *Ethernet SNAP* en1-snap.
Mode	Definiert den Modus, in dem die LAN-Schnittstelle betrieben wird. Mögliche Werte: ■ *Auto* (Standardwert): Automatische Erkennung der LAN-Parameter ist aktiviert, die LAN-Schnittstelle wird im passenden Modus betrieben. ■ *10 MBit Half Duplex* ■ *10 MBit Full Duplex* ■ *100 MBit Half Duplex* ■ *100 MBit Full Duplex* In der Regel sollten Sie den voreingestellten Wert *Auto* belassen.

Tabelle 6-5: ***CM-100BT, FAST ETHERNET***

ToDo Gehen Sie folgendermaßen vor, um die LAN-Schnittstelle von **X4100/200/300** zu konfigurieren:

➤ Geben Sie **local IP-Number** von **X4100/200/300** ein, z. B. ***192.168.1.254***.

➤ Geben Sie **local Netmask** ein, z. B. ***255.255.255.0***.

➤ Geben Sie gegebenenfalls **Second Local IP-Number** und **Second Local Netmask** ein.

➤ Wählen Sie **Encapsulation** aus, z. B. ***Ethernet II***.

➤ Wählen Sie **Mode** aus, z. B. ***Auto***.

➤ Bestätigen Sie mit **SAVE**.

Sie befinden sich wieder im Hauptmenü. Die Eintragungen sind temporär gespeichert und aktiviert.

Weiterführende Konfiguration

Informationen zu Bridging finden Sie in der **Software Reference**.

Im Menü ***CM-100BT, FAST ETHERNET*** ➧ ***ADVANCED SETTINGS*** finden Sie Einstellungen zum Routing Information Protocol RIP (siehe Kapitel 7.2.9, Seite 220), IP-Accounting, Proxy ARP (siehe Kapitel 7.2.11, Seite 224) und "Backroute Verification" (siehe Kapitel 9.2.10, Seite 356).

Wie Sie die zweite Ethernet-Schnittstelle der **X4100** und **X4200** oder eine LAN-Erweiterungskarte für xDSL konfigurieren, finden Sie in Kapitel 6.2.3, Seite 138 beschrieben.

6.1.4 X4100/200/300 als DHCP-Server einrichten

IP-Adressen im LAN

Jeder Rechner in Ihrem ➤➤ **LAN** benötigt, wie auch **X4100/200/300**, eine eigene IP-Adresse. Eine Möglichkeit, IP-Adressen in Ihrem LAN zuzuweisen, bietet das Dynamic Host Configuration Protocol (DHCP). Wenn Sie **X4100/200/300** als ➤➤ **DHCP**-Server einrichten, vergibt der Router anfragenden Rechnern im LAN automatisch ➤➤ **IP-Adressen** aus einem definierten IP-Adreß-Pool. Ein Rechner sendet einen ARP-Request aus und erhält daraufhin seine IP-Adresse von **X4100/200/300** zugewiesen. Sie müssen so 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 **X4100/200/300** 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-➤➤ **Gateways**.

DHCP-Server einrichten

Gehen Sie folgendermaßen vor:

➤ Gehen Sie zu ***IP*** ➧ ***IP ADDRESS POOL LAN (DHCP)*** ➧ **ADD**.

Folgendes Menüfenster öffnet sich:

```
X4x00 Setup Tool                              BinTec Access Networks GmbH
[IP][DHCP][ADD]: Add range of IP Addresses                      MyRouter


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

    Gateway
    NetBT Node Type                         not specified


                SAVE                            CANCEL

Use <Space> to select
```

Das Menü enthält folgende Felder:

Feld	Bedeutung
Interface	Schnittstelle, welcher 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 neu vergeben werden.
MAC Address	(optional) Nur bei **Number of consecutive addresses** = *1:* Nur dem Gerät mit **MAC Address** wird **IP Address** zugewiesen.

Feld	Bedeutung
Gateway	Legt fest, welche IP-Adresse dem DHCP-Client als Gateway übermittelt wird. Wenn hier keine IP-Adresse eingetragen wird, wird die IP-Adresse von **X4100/200/300** übertragen.
NetBT Node Type	Legt fest, wie und in welcher Reihenfolge für die Hosts eines Adreß-Pools die Zuordnung von NetBIOS-Namen zu IP-Adressen versucht wird. Sie können den Standardwert *not specified* übernehmen. Eine detaillierte Beschreibung dieser Funktion finden Sie in der **Software Reference**.

Tabelle 6-6: ***IP*** ➧ ***IP ADDRESS POOL LAN (DHCP)*** ➧ **ADD**

ToDo Nehmen Sie folgende Eintragungen vor, um **X4100/200/300** 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.
- Geben Sie gegebenenfalls **Gateway** ein.
- Wählen Sie **NetBT Node Type** aus, z. B. ***not specified***.
- Bestätigen Sie mit **SAVE**.

  Sie befinden sich im Menü ***IP*** ➧ ***IP ADDRESS POOL LAN (DHCP)***. Hier sind die IP-Adreß-Pools aufgelistet. Die Eintragungen sind gespeichert, Sie haben einen Adreßpool mit z. B. acht IP-Adressen definiert: 192.168.1.1 bis 192.168.1.8.

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..

6.1.5 Filter setzen

NetBIOS-Filter

Wenn Sie in Ihrem lokalen Netzwerk mit Windows arbeiten, sollten Sie ➤➤ **NetBIOS**-Filter setzen, um Kosten zu sparen. Dies verhindert, daß aus dem Netz Verbindungen z. B. zum Internet Service Provider (➤➤ **ISP**) aufbaut werden, um WINS-Requests von Rechnern in Ihrem Netzwerk weiterzugeben. D. h. **X4100/200/300** fragt beim ISP nach, welcher ➤➤ **Hostname** einer IP-Adresse zugeordnet werden kann. Da der ISP WINS-Namen nicht auflösen kann, sind diese Verbindungen unnötig, verursachen aber Kosten.

Ausführliche Erläuterungen zum Thema ➤➤ **Filter** und Sicherheit finden Sie in Kapitel 9.2.8, Seite 339.

ToDo

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 **X4100/200/300** zu.
- Wenn Sie trotzdem über Ihr LAN (z. B. telnet) auf **X4100/200/300** zugreifen, wählen Sie vor Beginn der Filter-Konfiguration im Menü ***IP*** ➧ ***ACCESS LISTS*** ➧ ***INTERFACES*** ➧ ***EDIT*** aus: **First Rule** = *none*.

- Gehen Sie zu ***IP*** ➧ ***ACCESS LISTS*** ➧ ***FILTER*** ➧ **ADD**.

Folgendes Menüfenster öffnet sich:

```
X4x00 Setup Tool                          BinTec Access Networks GmbH
[IP][ACCESS][FILTER][ADD]: Configure IP Access Filter         MyRouter

    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

    Type of Service (TOS)    00000000        TOS Mask     00000000

                    SAVE                     CANCEL

Enter string, max length = 48 chars
```

Filter für WINS-Request

Nehmen Sie folgende Eintragungen vor, um ein Filter für WINS-Requests 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.

Filterregeln Gehen Sie folgendermaßen vor, um die Regeln für die Filter festzulegen:

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

Folgendes Menü öffnet sich:

```
X4x00 Setup Tool                          BinTec Access Networks GmbH
[IP][ACCESS][RULE][ADD]: Configure IP Access Rules            MyRouter


    Action               deny M
    Filter               wrong_dns (1)


                SAVE                        CANCEL

Use <Space> to select
```

Erste Regel Nehmen Sie folgende Eintragungen vor, 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.

Zweite Regel 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:

```
X4x00 Setup Tool                          BinTec Access Networks GmbH
[IP][ACCESS][RULE]: Configure IP Access Rules                MyRouter

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>toedit
```

Interface zuordnen

Fahren Sie folgendermaßen fort:

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

Folgendes Menü öffnet sich:

```
X4x00 Setup Tool                          BinTec Access Networks GmbH
[IP][ACCESS][INTERFACES]: Configure First Rule               MyRouter

    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
```

➤ Wählen Sie die LAN-Schnittstelle von **X4100/200/300** (***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 DNS-Requests vom Quell-➤➤ **Port** 137 zum Ziel-Port 53 verworfen werden. 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. Die Eintragungen sind temporär gespeichert und aktiviert.

Zum Speichern der Konfiguration im Flash ist es notwendig, das Setup Tool mit **Save as boot configuration and exit** zu verlassen.

6.1.6 Wie geht's jetzt weiter?

Nachdem Sie **X4100/200/300** für Ihr LAN konfiguriert haben, können Sie die folgenden Schritte durchführen, um WAN-Verbindungen zu ermöglichen:

- Die WAN-Schnittstelle(n) von **X4100/200/300** konfigurieren, die Sie nutzen möchten (Kapitel 6.2, Seite 121).
- WAN-Partner konfigurieren (Kapitel 6.3, Seite 147).
- Wenn Sie mit dem **X4100/200/300**-Grundgerät Kommunikationsanwendungen auf den Hosts im LAN ermöglichen wollen, müssen Sie auf den Hosts die Remote-CAPI-Konfiguration durchführen (siehe Kapitel 6.5, Seite 177) und die Zuordnung der Rufnummern entsprechend durchführen ("Incoming Call Answering", Seite 125).
- Möglichkeiten für weiterführende Konfiguration finden Sie in Kapitel 7, Seite 179.
- Gegebenenfalls die Schnittstellen Ihrer Erweiterungskarte konfigurieren (Kapitel 8, Seite 287).

- Die Konfiguration von Sicherheitsfunktionen und Firewall finden Sie in Kapitel 9, Seite 311.

➤ Sichern Sie nach Beenden der Konfiguration auf jeden Fall Ihre Konfigurationsdatei (Kapitel 6.4, Seite 176).

6.2 WAN-Schnittstellen konfigurieren

Im folgenden finden Sie die Konfigurationsschritte, die zum Einrichten der WAN-Schnittstellen von **X4100/200/300** erforderlich sind, Schritt für Schritt beschrieben.

Die Grundgeräte von **X4100/200/300** verfügen über folgende WAN-Schnittstellen:

- ISDN-BRI-Schnittstelle (siehe Kapitel 6.2.1, Seite 121)
- X.21/V.35-Schnittstelle der **X4200** und **X4300** (seriell, Kapitel 6.2.2, Seite 133)

xDSL

- Sie können die zweite Ethernet-Schnittstelle von **X4100** und **X4200** bzw. eine LAN-Erweiterungskarte als WAN-Schnittstelle konfigurieren, indem Sie mit PPP-over-Ethernet oder PPTP eine Anbindung an einen xDSL-Anschluß ermöglichen (siehe Kapitel 6.2.3, Seite 138 für **X4100** und **X4200** bzw. für eine LAN-Erweiterungskarte).

Durch Einbau einer Erweiterungskarte können gegebenenfalls weitere WAN-Schnittstellen auf **X4100/200/300** genutzt werden, beachten Sie dazu Kapitel 8, Seite 287.

6.2.1 ISDN-BRI-Schnittstelle konfigurieren

Die ISDN-BRI-Schnittstelle von **X4100/200/300** können Sie sowohl für Wähl- als auch für Festverbindungen über ISDN nutzen.

Um die ISDN-BRI-Schnittstelle 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 **X4100/200/300** mit, wie auf eingehende Rufe aus dem WAN reagiert werden soll.

Einstellungen ISDN-Anschluß

Gehen Sie folgendermaßen vor, um die Einstellungen für Ihren ISDN-Anschluß vorzunehmen:

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

Folgendes Menü öffnet sich:

```
X4x00 Setup Tool                          BinTec Access Networks GmbH
[WAN]: WAN Interface                                        MyRouter

    Result of Autoconfiguration: Euro ISDN, point to multipoint
    ISDN Switch Type             autodetect on bootup

    D-Channel                    dialup
    B-Channel 1                  dialup
    B-Channel 2                  dialup

    Incoming Call Answering>
    Advanced Settings>

                     SAVE                      CANCEL

Use <Space> to select
```

Das Menü enthält 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.

Feld	Bedeutung
ISDN Switch Type	Definiert das ISDN-➤➤ **Protokoll**, das Ihnen Ihre Telefongesellschaft zur Verfügung stellt. Folgende Einstellungen sind möglich: ■ *autodetect on bootup:* automatische D-Kanalerkennung (Standardeinstellung) ■ *Euro ISDN point to multipoint:* Euro-ISDN an einem Mehrgeräteanschluß ■ *Euro ISDN point to point:* Euro-ISDN an einem Anlagenanschluß ■ *1TR6 point to multipoint* ■ *1TR6 point to point* ■ *National ISDN 1 AT&T NI1, EWSD NI1* ■ *AT&T 5ESS Custom ISDN point to multipoint* ■ *AT&T 5ESS Custom ISDN point to point* ■ *National ISDN 1 Northern Telecom DMS100* ■ *Japan NTT INS64* ■ *none* ■ *leased line B1 channel (64S):* Festverbindung über B-Kanal 1 ■ *leased line B1+B2 channel (64S2):* Festverbindung über beide B-Kanäle ■ *leased line D+B1+B2 channel (TS02):* Festverbindung über D-Kanal und beide B-Kanäle ■ *leased line B1+B2 different endpoints (Digital 64S mit Doppelanschaltung):* Festverbindung zu zwei verschiedenen Endpunkten

Feld	Bedeutung
D-Channel	Einstellung des D-Kanals. Eine Veränderung der Auswahl ist nur möglich bei **ISDN Switch Type** = *leased line D+B1+B2 (TS02)*. Mögliche Werte: ■ *leased dte* (Standardwert) ■ *leased dce*
B-Channel 1	Einstellung des ersten ➤➤ **B-Kanals**. Mögliche Werte: ■ *dialup* (Standardwert) ■ *not used* ■ *leased dte* ■ *leased dce*
B-Channel 2	Einstellung des zweiten B-Kanals. Mögliche Werte: ■ *dialup* (Standardwert) ■ *not used* ■ *leased dte* ■ *leased dce*

Tabelle 6-7: ***CM-1BRI, ISDN S0***

ToDo Nehmen Sie folgende Eintragungen vor:

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

Mit dieser Einstellung nutzt **X4100/200/300** 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***.

Bei einer Festverbindung oder 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!

In den meisten Fällen können Sie die voreingestellten Werte für **D-Channel**, **B-Channel 1** und **B-Channel 2** übernehmen.

Wenn Sie eine ISDN-Festverbindung nutzen und bei Ihrer Telefongesellschaft einen speziellen Service beantragt haben, kann es sein, daß hier die lokale Seite der Festverbindung entsprechend eingestellt werden muß (DTE oder DCE). Sie müssen dann darauf achten, daß die Gegenseite den gegenteiligen Wert eingestellt hat. Außerdem müssen Sie die Werte unter **D-channel**, **B-channel 1** und **B-channel 2** identisch einstellen, sofern Sie mehrere D-/B-Kanäle unter **ISDN Switch Type** augewählt haben und die Werte änderbar sind.

➤ Bestätigen Sie mit **SAVE**.

Sie befinden sich wieder im Hauptmenü. Die Eintragungen sind temporär gespeichert und aktiviert.

Incoming Call Answering

Falls Sie die ISDN-BRI-Schnittstelle für Wählverbindungen verwenden, müssen Sie als nächstes **X4100/200/300** die eigenen Rufnummern für diese Schnittstelle mitteilen (für Festverbindungen sind diese Einstellungen nicht möglich). Entsprechend den Einstellungen in den folgenden Menüs verteilt **X4100/200/300** die eingehenden Rufe auf die internen Dienste.

X4100/200/300 unterstützt die Dienste:

- PPP (Routing):
  Der Dienst ➤➤ **PPP** ist der allgemeine Routing-Dienst von **X4100/200/300**. Damit werden eingehenden Datenrufen von WAN-Partnern Wählverbindungen mit Ihrem ➤➤ **LAN** ermöglicht. So können Sie es Partnern außerhalb Ihres lokalen Netzwerkes ermöglichen, auf Hosts in Ihrem LAN zuzugreifen. Genauso ist es möglich, ausgehende Datenrufe zu WAN-Partnern außerhalb Ihres lokalen Netzwerks aufzubauen.

Dieses PPP-Routing wird auch für X.25-Verbindungen genutzt.

- ISDN-Login:
  Der Dienst ➤➤ **ISDN-Login** ermöglicht eingehenden Datenrufen Zugang zur ➤➤ **SNMP-Shell** von **X4100/200/300**. So kann **X4100/200/300** aus der Ferne konfiguriert und gewartet werden.

- CAPI:
  Der Dienst ➤➤ **CAPI** ermöglicht eingehenden und ausgehenden Daten- und Sprachrufen die Verbindung mit Kommunikationsanwendungen auf Hosts im LAN, die auf die ➤➤ **Remote-CAPI**-Schnittstelle von **X4100/200/300** zugreifen. So können beispielsweise mit **X4100/200/300** verbundene Hosts Faxe empfangen und senden.
  Um mit dem **X4100/200/300**-Grundgerät CAPI-Applikationen von den Hosts im LAN aus nutzen zu können, müssen Sie außer der in diesem Kapitel beschriebenen Rufnummernverteilung auch die Remote-CAPI-Konfiguration auf den einzelnen Hosts durchführen (siehe Kapitel 6.5, Seite 177).

Hier eine grafische Darstellung der Diensteverteilung:

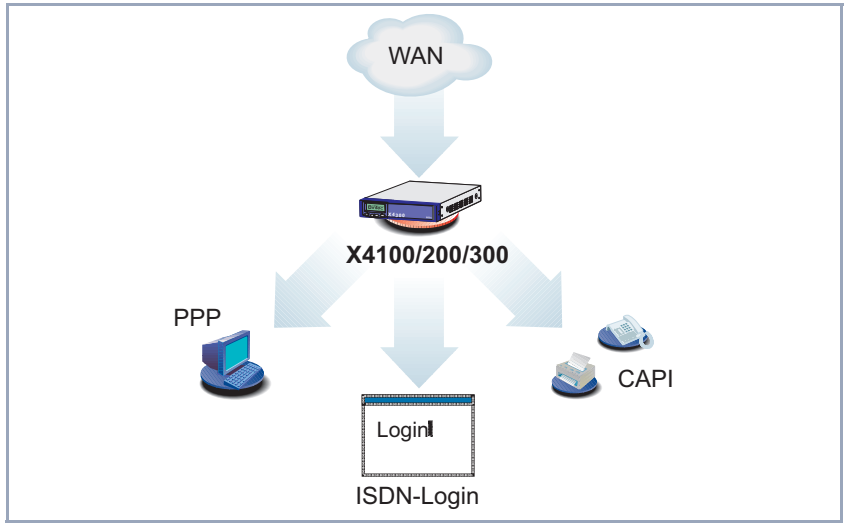


Bild 6-3: Verteilung der eingehenden Rufe

Wenn ein Ruf eingeht, überprüft **X4100/200/300** zunächst die Called Party Number (CPN) und die Art des Anrufs (Daten- oder Sprachruf). CPN ist die Rufnummer, die der Partner gewählt hat, um **X4100/200/300** zu erreichen. Anschließend wird der Ruf an den passenden Dienst weitergeleitet (siehe Bild 6-3, Seite 127).

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 6-8: Verteilung der Rufnummern auf Dienste

Wenn Sie im folgenden Menü keine Eintragungen vornehmen, wird jeder über ISDN eingehende Ruf vom 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 den entsprechenden Diensten zugeteilt.

Im Auslieferungszustand ist für das Subsystem CAPI immer ein Benutzer mit dem Benutzernamen "default" ohne Paßwort eingetragen. Alle Rufe an die CAPI werden somit allen CAPI-Applikationen im LAN angeboten.

Um die eingehenden Rufe für das Subsystem CAPI auf definierte User mit Paßwort zu verteilen, sollten Sie BinTecs User Concept nutzen (siehe Kapitel 7.1.2, Seite 182). Den Benutzer "default" ohne Paßwort sollten Sie dann löschen.

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

Incoming Call Answering eintragen

Nehmen Sie nun die Eintragungen für Incoming Call Answering vor:

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

In diesem Menü sind die bisher vorgenommenen Zuteilungen der Dienste zu den Rufnummern aufgelistet:

```
X4x00 Setup Tool                          BinTec Access Networks GmbH
[WAN][INCOMING]: Incoming Call Answering                     MyRouter


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/untagDELETE,<Return>to edit
```

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 öffnet sich:

```
X4x00 Setup Tool                          BinTec Access Networks GmbH
[WAN][INCOMING][ADD]: Incoming Calls                          MyRouter


    Item                    PPP (routing)
    Number                  10
    Mode                    right to left

    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. Mögliche Werte: siehe Tabelle 6-10, Seite 131.
Number	Rufnummer, unter welcher der oben eingetragene Dienst (**Item**) erreicht werden kann.
Mode	Modus, mit dem **X4100/200/300** den Ziffernvergleich von **Number** mit der Called Party Number des eingehenden Rufes durchführt: ■ *right to left* (Standardwert) ■ *left to right (DDI):* Immer auswählen, wenn **X4100/200/300** mit einem Point-to-Point-Anschluß (Anlagenanschluß) verbunden ist.

Feld	Bedeutung
Username	(nur bei **Item** = *CAPI 1.1 EAZ 0...9 Mapping*) CAPI-Benutzername. Nur erforderlich, wenn Sie das CAPI User Concept nutzen wollen (siehe Kapitel 7.1.2, Seite 182).
Bearer	Art des eingehenden Rufes. Mögliche Werte: ■ *data:* Datenruf ■ *voice:* Sprachruf ■ *any:* sowohl Daten- als auch Sprachruf

Tabelle 6-9: ***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 kBit/s PPP-Datenverbindungen.
PPP 56k	Ermöglicht 56 kBit/s PPP-Datenverbindungen.
PPP Modem	(nur verfügbar bei eingebauter Erweiterungskarte mit Ressourcenkarte mit Digitalmodems) Weist eingehende analoge Rufe dem Dienst PPP-Routing zu. Das digitale Modem auf der Ressourcenkarte, das diesen Ruf entgegennimmt, verwendet die Einstellungen von Modemprofil 1, die im Menü ***MODEM*** ➧ ***PROFILE CONFIGURATION*** ➧ ***PROFILE 1*** getroffen wurden.

Mögliche Werte	Bedeutung
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 und mit Bit-Raten von 1200 Bit/s, 2400 Bit/s,..., 38400 Bit/s.
Pots	Auf **X4100/200/300** nicht verfügbar.
PPP Modem Profile 1...8	(nur verfügbar bei eingebauter Erweiterungskarte mit Ressourcenkarte mit Digitalmodems) Weist eingehende analoge Rufe dem Dienst PPP-Routing zu. Das digitale Modem auf der Ressourcenkarte, das diesen Ruf entgegennimmt, verwendet die Einstellungen der Modemprofile 1 bis 8, die im Menü ***MODEM*** ➧ ***PROFILE CONFIGURATION*** ➧ ***PROFILE 1...8*** getroffen wurden.
CAPI 1.1 EAZ 0...9 Mapping	Ermöglicht Verbindungen mit Remote-CAPI-Applikationen. Nur erforderlich für CAPI 1.1-Applikationen.
X.25 PAD	Ermöglicht Datenverbindungen mit X.25 PAD.
CAPI 2.0	Ermöglicht Verbindungen mit Remote-Capi-Applikationen. Nur für Capi-2.0-Applikationen.

Tabelle 6-10: **Item**

Achten Sie darauf, unter **Number** die richtige Nummer, d. h. die Nummer, die auch wirklich bei **X4100/200/300** ankommt, einzutragen! Wenn **X4100/200/300** z. B. an einer ➤➤ **TK-Anlage** angeschlossen ist, kommt nur die Nebenstellennummer bei **X4100/200/300** an.

Wenn Sie sich nicht sicher sind, welche Nummer bei **X4100/200/300** wirklich ankommt, gehen Sie folgendermaßen vor:

- Rufen Sie mit einem herkömmlichen Telefon **X4100/200/300** 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 **X4100/200/300** ankommt.
- Geben Sie diesen Anteil der Rufnummer in ***CM-1BRI, ISDN S0*** ➧ ***INCOMING CALL ANSWERING*** ➧ **ADD** unter **Number** ein.

Falls Sie auf Ihrem Rechner mit einer Kommunikationsanwendung arbeiten, die auf Remote-CAPI 1.1 aufsetzt (aktuell: Remote-CAPI 2.0), muß **X4100/200/300** die ➤➤ **MSN** (=**Number**, mehrstellig) des eingehenden Rufes in ➤➤ **EAZ** (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, jeder CAPI-Anwendung die passende(n) EAZ(s) per "mapping" zuzuteilen. Wählen Sie 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*.

Mit CAPI 2.0 wird die MSN direkt ausgewertet, eine "Übersetzung" zu EAZ ist nicht notwendig. Sie sollten auf jeden Fall versuchen, Ihr Rechnersystem auf CAPI 2.0 umzustellen, um auch neue Leistungsmerkmale nutzen zu können.

Rufnummern den Diensten zuordnen

Nehmen Sie folgende Eintragungen vor:

- 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. Wenn also ein Datenruf an die Called Party Number 10 eingeht, wird er an den Dienst PPP (routing) weitergeleitet.
- Wiederholen Sie diese Schritte, bis Sie allen Rufnummern die Dienste zugeordnet haben, die unter diesen Rufnummern erreichbar sein sollen.

  Damit haben Sie Incoming Call Answering konfiguriert, **X4100/200/300** verteilt alle eingehenden Rufe an die internen Dienste.

Weiterführende Konfiguration

Unter ***CM-1BRI, ISDN S0*** ➧ ***ADVANCED SETTINGS*** finden Sie Einstellungen für X.31-TEI (siehe Kapitel 7.1.4, Seite 188).

Falls Sie eine Festverbindung nutzen, können Sie mit dem Feature "Bandwidth on Demand" u. a. eine Backup-Lösung realisieren (siehe Kapitel 7.2.3, Seite 193). Wenn Sie diese Möglichkeit nutzen, wird bei Ausfall der Festverbindung eine Wählverbindung zum Verbindungspartner aufgebaut.

6.2.2 Serielle WAN-Schnittstellen konfigurieren für X4200 und X4300

Die Grundgeräte von **X4200** und **X4300** verfügen über eine bzw. zwei serielle WAN-Schnittstellen des Typs:

- X.21/V.11
- V.35/V.11

Konfiguration mit dem Setup Tool

Die Konfiguration der X.21/V.35-Schnittstelle von **X4200** bzw. **X4300** erfolgt im Menü ***CM-SERIAL,SERIAL*** ➧ ***UNIT 0***:

```
X4x00 Setup Tool                          BinTec Access Networks GmbH
[SLOT 3 UNIT 0 SERIAL]: Configure Serial Interface           MyRouter


    Interface Type       X.21
    Connector            dte
    Clock mode           auto
    Speed                64000 bit/s
    Layer 2 Mode         auto

    Interface Leads      disabled


                SAVE                        CANCEL

Use <Space> to select
```

Das Menü hat folgende Felder:

Feld	Bedeutung
Interface Type	Definiert den Schnittstellentyp des verwendeten Ports. Mögliche Werte: ■ *none* (Standardwert): Schnittstelle wird nicht genutzt. ■ *X.21*: Nutzung als X.21/V.11-Schnittstelle ■ *V.35*: Nutzung als V.35/V.11-Schnittstelle

Feld	Bedeutung
Connector	Legt die Pinbelegung des Ports fest (siehe Kapitel 12.2.5, Seite 404). Nur beim ersten seriellen Port ***CM-SERIAL, SERIAL ➧ UNIT 0*** kann durch diese Einstellung die Pinbelegung beeinflußt werden, beim zweiten seriellen Port ***CM-SERIAL, SERIAL ➧ UNIT 1*** muß ein entsprechendes DCE- bzw. DTE-Kabel verwendet werden! Mögliche Werte: ■ *dte* (Standardwert): Die Pins sind als DTE-Schnittstelle belegt. Diese Einstellung ist z. B. dann erforderlich, wenn **X4100/200/300** mit einem öffentlichen Datennetz verbunden ist (z. B. Datex-P in Deutschland). ■ *dce*: Die Pins sind als DCE-Schnittstelle belegt. Dies ist erforderlich, um ein DTE-konfiguriertes Gerät bedienen zu können.

Feld	Bedeutung
Clock Mode	Definiert, welcher Verbindungspartner das Taktsignal zur Synchronisation zwischen Sender und Empfänger gibt. Mögliche Werte: ■ *auto* (Standardwert): Die Einstellung richtet sich nach der für **Connector** getroffenen Auswahl: – **X4100/200/300** gibt das Taktsignal, wenn **Connector** = *dce*. – **X4100/200/300** empfängt das Taktsignal, wenn **Connector** = *dte*. In der Regel können Sie diese Einstellung übernehmen. ■ *extern*: **X4100/200/300** empfängt das Taktsignal, unabhängig von der unter **Connector** gewählten Einstellung. ■ *intern*: **X4100/200/300** gibt das Taktsignal, unabhängig von der unter **Connector** gewählten Einstellung.
Speed	Übertragungsrate der Verbindung, skalierbar von *2400 bit/s* bis *8 Mbit/s*. Der einzustellende Wert ist abhängig von Qualität und Länge des Kabels und vom Verbindungstyp (symmetrisch/asymmetrisch). Über eine kurze Distanz von bis zu 5 m und bei Verwendung von abgeschirmten Kabeln sind bis zu 8 Mbit/s möglich. Standardwert: *64000 bit/s*

Feld	Bedeutung
Layer 2 Mode	Definiert den Wert des HDLC-Adreßfelds in gesendeten Kommando-Frames (Schicht 2). Mögliche Werte: ■ *auto* (Standardwert): Die für **Connector** getroffene Auswahl wird übernommen. In der Regel können Sie diese Einstellung übernehmen, z. B. auch bei Zugang zu einem öffentlichen Datennetz (z. B. Datex-P). ■ *dte:* Das Adressfeld hat den Wert für DTE. ■ *dce:* Das Adressfeld hat den Wert für DCE.
Interface Leads	Legt fest, ob **X4100/200/300** den Status der Schnittstellenleitung überprüft. Bei beiden Verbindungspartnern sollte der gleiche Wert eingestellt sein. Mögliche Werte: ■ *enabled:* Der Status der Signalleitung (I bei X.21, CTS bei V.35) wird überprüft und als **L1State** übernommen. ■ *disabled* (Standardwert): Der Status wird nicht überprüft, die physikalische Leitung ist immer up. Bei dieser Einstellung sollten Sie die Schnittstellenleitung auf andere Weise überwachen, z. B. durch PPP-Keepalive.

Tabelle 6-11: ***CM-SERIAL, SERIAL*** ➧ ***UNIT 0*** bzw. ***CM-SERIAL, SERIAL*** ➧ ***UNIT 1***

ToDo Gehen Sie folgendermaßen vor, um die seriellen WAN-Schnittstellen von **X4200** und **X4300** zu konfigurieren (die angegebenen Beispielswerte sind erforderlich, wenn Sie den Router an Datex-P anschließen):

➤ Gehen Sie zu ***CM-SERIAL,SERIAL*** ➧ ***UNIT 0*** bzw. ***CM-SERIAL,SERIAL*** ➧ ***UNIT 1***.

➤ Wählen Sie **Interface Type** aus: z. B. ***X.21***.

➤ Wählen Sie **Connector** aus: z. B. ***dte***.

- Wählen Sie **Clock Mode** aus: z. B. ***auto***.
- Wählen Sie **Speed** aus: z. B. ***64000 bit/s***.
- Wählen Sie **Layer 2 Mode** aus: z. B. ***auto***.
- Wählen Sie **Interface Leads** aus: z. B. ***disabled***.
- Bestätigen Sie mit **SAVE**.

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

Weiterführende Konfiguration

Falls Sie eine Festverbindung nutzen, können Sie mit dem Feature "Bandwidth on Demand" u. a. eine Backup-Lösung realisieren (siehe Kapitel 7.2.3, Seite 193). Wenn Sie diese Möglichkeit nutzen, wird bei Ausfall der Festverbindung eine Wählverbindung zum Verbindungspartner aufgebaut.

6.2.3 Breitband-Internetzugang (xDSL) mit X4100 und X4200 oder LAN-Erweiterungskarte

BinTec Access Networks GmbH bietet mit **X4100/200/300** die Protokolle PPP-over-Ethernet und PPTP an. Diese Protokolle werden benötigt, um z. B. Endgeräte über einen xDSL-Anschluß mit dem Internet zu verbinden und somit eine erhöhte Bandbreite zu erreichen.

Wenn Sie den xDSL-Anschluß eines anderen Providers als der Deutschen Telekom nutzen, erkundigen Sie sich gegebenenfalls beim Provider über die zu beachtenden Besonderheiten Ihres xDSL-Anschlusses.

Beispiel 1: Deutsche Telekom

Hier das Szenario der folgenden Beispielkonfiguration:

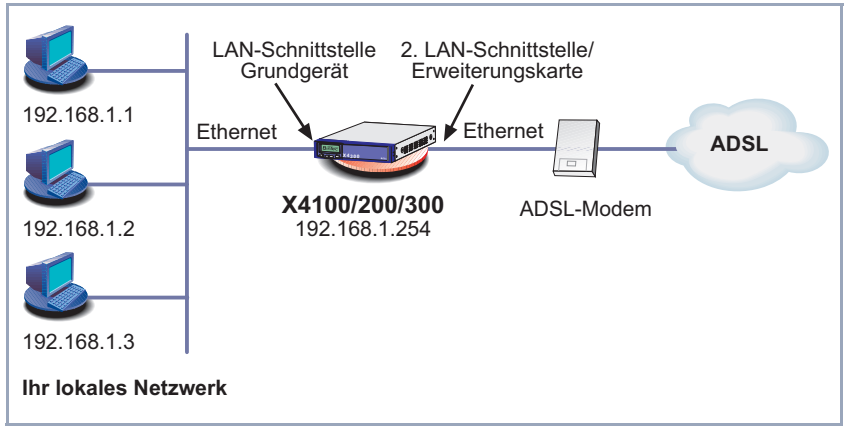


Bild 6-4: Beispielszenario

Der LAN-Anschluß wird über die LAN-Schnittstelle des **X4100/200/300**-Grundgeräts abgewickelt. Das xDSL-Modem wird dem 10-Base-T-Ethernet-Anschluß (nur **X4100** und **X4200**) oder mit einer der LAN-Schnittstellen der Erweiterungskarte (X4E-2 FE) verbunden.

Sollten Sie von der Deutschen Telekom AG oder einem anderen Provider für den Anschluß des xDSL-Modems ein spezielles Kabel erhalten, verwenden Sie nur dieses Kabel!

IP-Adresse konfigurieren

Gehen Sie folgendermaßen vor, um die IP-Adresse von **X4100/200/300** festzulegen (falls noch nicht geschehen, wie in Kapitel 6.1.3, Seite 108):

- Gehen Sie zu ***X4E-100BT, FAST ETHERNET***.
- Geben Sie im Feld **local IP-Number** Ihre IP-Adresse ein, z. B. ***192.168.1.254***.
- Geben Sie im Feld **local Netmask** Ihre Netzmaske ein, z. B. ***255.255.255.0***.
  Diese Adresse sollte Default-Gateway für die Hosts in Ihrem LAN sein.
- Bestätigen Sie mit **SAVE**.

Allgemeine PPP-Einstellungen

Die Konfiguration der allgemeinen PPP-Einstellungen erfolgt im Menü ***PPP***.

Hier müssen Sie ein Interface konfigurieren, auf dem PPP-over-Ethernet laufen soll. Alle anderen Einstellungen können Sie in der Voreinstellung belassen.

➤ Gehen Sie zu ***PPP***.

Folgendes Feld ist hierbei relevant:

Feld	Bedeutung
PPPoE Ethernet Interface	Definiert das Interface, über welches xDSL läuft.

Tabelle 6-12: ***PPP***

Gehen Sie folgendermaßen vor, um die notwendigen PPP-Einstellungen festzulegen:

➤ Wählen Sie Ihr **PPPoE Ethernet Interface** aus, z. B. ***en2*** (2. LAN-Schnittstelle in Bild 6-4, Seite 139).

➤ Bestätigen Sie mit **SAVE**.

WAN-Partner-Einstellungen

Um einen PPP-over-Ethernet-Partner zu konfigurieren, gehen Sie genau so vor, wie bei der WAN-Partner-Konfiguration.

Bitte achten Sie bei der WAN-Partner-Konfiguration darauf, daß Van-Jacobson-Header-Komprimierung im Menü ***WAN PARTNER*** ➧ ***ADD*** ➧ ***IP*** ➧ ***ADVANCED SETTINGS*** nicht aktiviert ist. Ebenso können die Funktionen Bridging und "Bandwidth on Demand" nicht genutzt werden.

➤ Gehen Sie zu ***WAN PARTNER*** ➧ ***ADD***.

Folgende Felder sind hierbei relevant:

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

Feld	Bedeutung
Encapsulation	Enkapsulierung. Definiert, wie die Datenpakete für die Übertragung zum WAN-Partner verpackt werden. Bei PPP-over-Ethernet: Hierbei sollte nur *PPP* ausgewählt werden.

Tabelle 6-13: ***WAN PARTNER*** ➧ ***ADD***

➤ Tragen Sie unter **Partner Name** Ihren PPP-over-Ethernet WAN-Partner-Namen ein, z. B. ***t-online***.

➤ Wählen Sie **Encapsulation** aus: *PPP*.

WAN-Partner-PPP-Einstellungen

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

Folgende Felder sind hierbei relevant:

Feld	Bedeutung
Partner PPP ID	Kennung des WAN-Partners. Bleibt hier leer.
Local PPP ID	Ihre T-Online User-ID. Setzt sich folgendermaßen zusammen: <Kennung><T-Online-Nr.>#<Mitben.-Nr.>@t-online.de. Kennung = Die zwölfstellige Anschlußkennung (Beispiel: ***000460004256***) T-Online-Nr. = Telefonnummer (Beispiel: ***091169386***) Mitben.-Nr. = vierstellige Mitbenutzernummer (Beispiel: ***0001***) Die T-Online-Nummer und die Mitbenutzer-nummer müssen durch # getrennt werden, wenn die T-Online-Nummer weniger als 12 Stellen hat.
PPP Password	Ihr T-Online-Paßwort.

Feld	Bedeutung
Keepalives	Aktiviert Keepalive-Pakete. Die aktivierte Keepalive-Funktion prüft den Interface-Status. So kann schneller erkannt und signalisiert werden, wenn die Verbindung zum Provider ausfällt (falls beispielsweise versehentlich das LAN-Kabel abgezogen wurde).

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

- Nehmen Sie unter **Partner PPP ID** keine Eintragung vor.
- Tragen Sie **Local PPP ID** ein,
  z. B. ***00046000425609116938 6#0001@t-online.de***.
- Tragen Sie **PPP Password** ein.
- Wählen Sie **Keepalives** aus: *on*.
- Bestätigen Sie mit **OK**.

Advanced Settings

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

Folgendes Feld ist hierbei relevant:

Feld	Bedeutung
Layer 1 Protocol	Für den Zugang zu xDSL muß hier *PPP over Ethernet (PPPoE)* ausgewählt werden.

Tabelle 6-15: ***WAN PARTNER*** ➧ ***ADD*** ➧ ***ADVANCED SETTINGS***

- Wählen Sie **Layer 1 Protocol** aus: *PPP over Ethernet (PPPoE)*.
- Bestätigen Sie mit **OK**.

IP-Einstellungen

- Gehen Sie zu ***WAN*** ➧ ***ADD*** ➧ ***IP***.

Folgendes Feld ist hierbei relevant:

Feld	Bedeutung
IP Transit Network	Legt fest, ob **X4100/200/300** ein Transit-Network zum WAN-Partner nutzt. Die IP-Adresse wird dynamisch zugewiesen, wenn *dynamic client* ausgewählt ist.

Tabelle 6-16: ***WAN PARTNER*** ➧ ***ADD*** ➧ ***IP***

- Wählen Sie **IP Transit Network** aus: *dynamic client*.
- Bestätigen Sie mit **SAVE**.
- Bestätigen Sie mit **SAVE**.
- Verlassen Sie ***WAN PARTNER*** mit **EXIT**.

Default-Route anlegen

- Gehen Sie zu ***IP*** ➧ ***ROUTING*** ➧ ***ADD***.

Folgendes Feld ist hierbei relevant:

Feld	Bedeutung
Partner / Interface	Ihr PPPoE Partner.

Tabelle 6-17: ***IP*** ➧ ***ROUTING*** ➧ ***ADD***

- Wählen Sie **Route Type** aus: *Default route*.
- Wählen Sie **Partner / Interface** aus, z. B. ***t-online***.
- Bestätigen Sie mit **SAVE**.

Network Address Translation (NAT) aktivieren

Mit NAT erreichen Sie folgendes:

- Aus dem Internet kann nicht mehr auf Ihr Netz zugegriffen werden.
- Verbindungen ins Internet erscheinen nur unter der einen, dynamisch zugeteilten IP-Adresse.

- Gehen Sie zu ***IP*** ➧ ***NETWORK ADDRESS TRANSLATION***.

➤ Wählen Sie das WAN-Interface aus, auf dem Sie NAT aktivieren möchten, z. B. ***t-online***, und bestätigen Sie mit der **Eingabetaste**.

Ein weiteres Menü öffnet sich.

Folgendes Feld ist hierbei relevant:

Feld	Bedeutung
Network Address Translation	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.

Tabelle 6-18: ***IP*** ➧ ***NAT***

➤ Wählen Sie **Network Address Translation** aus: *on*.

➤ Bestätigen Sie mit **SAVE**.

Die WAN-Schnittstelle für T-DSL ist konfiguriert.

Beispiel 2: Telekom Austria (High-Speed-Internet-Anschluß)

Telekom Austria bietet einen Hochgeschwindigkeitszugang zum Internet (A-Online Speed), der z. B. in Österreich verfügbar ist. Gehen Sie folgendermaßen vor:

WAN-Partner einrichten

➤ Gehen Sie zu ***WAN PARTNER*** ➧ **ADD**.

➤ Geben Sie **Partner Name** (= Provider-Name) ein: *Telekom_Austria*.

➤ Wählen Sie **Encapsulation** aus: *PPP*.

➤ Wählen Sie **Compression** aus: *none*.

➤ Wählen Sie **Encryption** aus: *none*.

PPP-Authentisierung festlegen

➤ Wählen Sie **PPP** aus und bestätigen Sie mit der **Eingabetaste**.

➤ Wählen Sie **Authentication** aus: *CHAP*.

➤ **Partner PPP ID** brauchen Sie nicht einzugeben. Das Feld bleibt leer.

➤ Geben Sie **Local PPP ID** (= Ihr Benutzername) ein, z. B. ***3909987000***.

➤ 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. *90*. (Wenn Sie eine Flat-Rate Verbindung nutzen, können Sie **Static Short Hold (sec)** *-1* eingeben.)
- Geben Sie **Idle for Dynamic Short Hold (%)** ein: *0*.
- Geben Sie **Delay after Connection Failure (sec)** ein, z. B. ***300***.
- Wählen Sie **Layer 1 Protocol** aus: *PPP over PPTP*.
- Überspringen Sie **Extended Interface Settings**.
- 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**.
- Geben Sie **VPN Partner's IP Address** ein: *10.0.0.138*.
- Wählen Sie **via IP Interface** aus: z. B ***en2*** (2. LAN-Schnittstelle in Bild 6-4, Seite 139).
- Geben Sie **local IP Address** ein: *10.0.0.140*.
- Überspringen Sie **Advanced Settings**.
- Bestätigen Sie mit **SAVE**.

  Sie befinden sich wieder im Menü ***WAN PARTNER*** ➧ **ADD**.
- Bestätigen Sie 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: *Telekom_Austria*.
- Geben Sie **Metric** ein, z. B. ***1***.
- Bestätigen Sie mit **SAVE**.
- Verlassen Sie ***IP*** ➧ ***ROUTING*** mit **EXIT**.

  Sie befinden sich im Menü ***IP***.

NAT aktivieren

- Gehen Sie zu ***IP*** ➧ ***NETWORK ADDRESS TRANSLATION***.
- Wählen Sie das IP Interface Telekom_Austria 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 Hochgeschwindigkeitszugangs ist abgeschlossen.

6.3 WAN-Partner konfigurieren

Um mit **X4100/200/300** Verbindungen zu Netzwerken oder Hosts außerhalb Ihres LANs herstellen zu können, müssen Sie die gewünschten Verbindungspartner als WAN-Partner auf **X4100/200/300** einrichten. Dies gilt sowohl für ausgehende Verbindungen (**X4100/200/300** wählt sich bei einem WAN-Partner ein), als auch für eingehende Verbindungen (ein WAN-Partner wählt sich bei **X4100/200/300** ein) und Festverbindungen.

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

Wenn Sie bei der Konfiguration der WAN-Schnittstelle(n) von **X4100/200/300** eine oder mehrere Festverbindungen eingerichtet haben, wird im Menü ***WAN PARTNER*** bereits automatisch jeweils ein WAN-Partner für eine Festverbindung angelegt. Editieren Sie diesen Eintrag entsprechend Ihren Erfordernissen.

Wenn Sie einen Internetzugang über Compuserve einrichten möchten, beachten Sie bitte "Internetzugang über Compuserve", Seite 174.

Prinzipielle Vorgehensweise

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

- WAN-Partner einrichten (Kapitel 6.3.1, Seite 148)
  - ➤➤ **Protokoll** (Enkapsulierung) festlegen.
  - Rufnummer(n) eintragen.
  - ➤➤ **PPP**-Einstellungen zur Authentisierung festlegen.
  - ➤➤ **Shorthold** festlegen.
  - IP-Konfiguration durchführen.
- Routing-Eintrag erstellen (Kapitel 6.3.2, Seite 165)
- Network Address Translation (➤➤ **NAT**) aktivieren (optional, Kapitel 6.3.3, Seite 171)

Beispiele In Kapitel 6.3.4, Seite 172 sind einige häufig benötigte Konfigurationsbeispiele dargestellt.

6.3.1 WAN-Partner einrichten

Legen Sie sich gegebenenfalls die notwendigen Zugangsdaten, die Sie von Ihrem ISP oder Systemadministrator erhalten haben, zurecht (siehe Kapitel 4.5.1, Seite 79). Die Bezeichnungen können unter Umständen von Provider zu Provider leicht variieren.

WAN-Partner einrichten

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

➤ Gehen Sie zu ***WAN PARTNER***.

Hier sind die aktuell eingetragenen WAN-Partner mit **Partnername**, **Protocol** und **State** aufgelistet:

```
X4x00 Setup Tool                          BinTec Access Networks GmbH
[WAN]: WAN Partners                                          MyRouter

Current WAN Partner Configuration

    Partnername             Protocol        State
    LittleIndian            ppp             dormant



ADD                 DELETE              EXIT


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

Für Festverbindungen wird automatisch ein WAN-Partner-Interface angelegt. Editieren Sie den vorangelegten Eintrag für eine Festverbindung im Menü ***WAN PARTNER*** und geben Sie die erforderlichen Parameter ein.

State kann folgende Werte annehmen:

Mögliche Werte	Bedeutung
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)
down	administrativ auf *down* gesetzt

Tabelle 6-19: **State**

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 öffnet sich:

```
X4x00 Setup Tool                          BinTec Access Networks GmbH
[WAN][ADD]:Configure WAN Partner                                MyRouter

    Partner Name                 LittleIndian

    Encapsulation                PPP
    Encryption                   none
    Compression                  none
    Calling Line Identification  no

    WAN Numbers >
    PPP >
    Advanced Settings >

    IP >
    Bridge >

                     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.
Encapsulation	➤➤ **Enkapsulierung**. Definiert, wie die ➤➤ **Daten-Pakete** für die Übertragung zum WAN-Partner verpackt 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* ■ *X.25* ■ *HDLC Framing (only IP)* ■ *LAPB Framing (only IP)* ■ *X31 B-Channel* ■ *X.25 No Signalling* ■ *X.25 PAD* ■ *X.25 No Configuration* ■ *Frame Relay* ■ *X.25 No Configuration, No Signalling*

Feld	Bedeutung
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:* MPPE Version 1 mit 40-Bit-Schlüssel ■ *MPPE 56:* MPPE Version 1 mit 56-Bit-Schlüssel ■ *MPPE 128:* MPPE Version 1 mit 128-Bit-Schlüssel ■ *MPPE V2 40:* MPPE Version 2 mit 40-Bit-Schlüssel ■ *MPPE V2 56:* MPPE Version 2 mit 56-Bit-Schlüssel ■ *MPPE V2 128:* MPPE Version 2 mit 128-Bit-Schlüssel ■ *DES 56*: DES mit 56-Bit-Schlüssel ■ *Blowfish 56*: Blowfish mit 56-Bit-Schlüssel ■ *none:* keine Verschlüsselung Diese Werte sind nur verfügbar, wenn unter **Encapsulation** *PPP*, *Async PPP over X.75*, *Async PPP over X.75/T.70/BTX* oder *X.25_PPP* ausgewählt wurde.
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* ■ *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 6-20: ***WAN PARTNER*** ➧ **ADD**

Folgende ➤➤ **Datenkomprimierung**en werden von den Enkapsulierungen unterstützt:

Enkapsulierung	Komprimierung: STAC, MS-STAC
PPP	X
Async PPP over X.75	X
Async PPP over X.75/ T.70/BTX	X

Tabelle 6-21: Enkapsulierung und Komprimierung

Protokoll festlegen

ToDo Nehmen Sie folgende Eintragungen vor:

- Geben Sie **Partner Name** ein, z. B. ***LittleIndian***.
- Wählen Sie **Encapsulation** aus, z. B. ***PPP***.
- Wählen Sie gegebenenfalls **Compression** aus, z. B. ***none***.
- Wählen Sie gegebenenfalls **Encryption** aus, z. B. ***none***.

Rufnummern eintragen

Gehen Sie folgendermaßen vor, um die Rufnummern des WAN-Partners einzutragen:

- Gehen Sie zu ***WAN PARTNER*** ➧ **ADD** ➧ ***WAN NUMBERS***.

In diesem Menü sind die aktuell eingetragenen Rufnummern des WAN-Partners aufgelistet:

```
X4x00 Setup Tool                          BinTec Access Networks GmbH
[WAN][ADD][WAN Numbers]: WAN Numbers (BigBoss)                MyRouter


    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>toedit
```

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 öffnet sich:

```
X4x00 Setup Tool                          BinTec Access Networks GmbH
[WAN][ADD][WANNUMBERS][ADD]: Add or Change WANNumbers(BigBoss)MyRouter


    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.

Feld	Bedeutung
Direction	Definiert, ob **Number** für eingehende oder für ausgehende Rufe oder für beides verwendet werden soll.
ISDN Ports to use	(Nur mit ISDN-Erweiterungskarten) Definiert die zu verwendenden ISDN-Ports.

Tabelle 6-22: ***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 **X4100/200/300** einwählen soll.

Tabelle 6-23: Direction

Wenn **X4100/200/300** an eine TK-Anlage angeschlossen ist, bei der für eine Amtsholung eine führende "0" gewählt wird, müssen Sie diese führende Null bei der Einwahlnummer berücksichtigen.

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

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

Wildcard	Bedeutung		Beispiel		
	Eingehende Rufe	Ausgehende Rufe	Number	X4100/200/300 akzeptiert eingehende Rufe z. B. mit:	Ausgehende Rufe, d. h. X4100/200/300 baut eine Verbindung zum WAN-Partner auf mit:
*	Entspricht einer Gruppe von keiner bis mehreren Ziffern.	Wird ignoriert.	123*	123, 1234, 123789	123
?	Entspricht genau einer Ziffer.	Wird durch 0 ersetzt.	123?	1234, 1238, 1231	1230
[a-b]	Definiert einen Bereich von passenden Ziffern.	Die erste Ziffer des definierten Bereiches wird verwendet.	123[5-9]	1235, 1237, 1239	1235
[^a-b]	Definiert einen Bereich von verbotenen Ziffern.	Die erste Ziffer nach dem definierten Bereich wird verwendet.	123[^0-5]	1236, 1238, 1239	1236
{ab}	Entspricht einer Gruppe von optionalen Ziffern.	Wird verwendet.	{00}1234	001234 und 1234	001234

Tabelle 6-24: 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 Nehmen Sie die folgenden Eintragungen vor:

- 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-Einstellungen zur Authentisierung festlegen

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 **X4100/200/300** 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, anschließend tragen Sie ein gemeinsames Paßwort und zwei Kennungen ein. Diese Daten erhalten Sie z. B. von Ihrem Internet Service Provider oder dem Systemadministrator der Firmenzentrale. Stimmen die von Ihnen auf **X4100/200/300** eingetragenen Daten mit den Daten des Anrufers überein, wird der Ruf angenommen. Stimmen die Daten nicht überein, wird der Ruf abgewiesen.

Wenn Sie WAN-Partner über einen RADIUS-Server authentisieren, beachten Sie bitte die entsprechenden Hinweise in der **Software Reference**.

PPP-Authentisierung des WAN-Partners festlegen

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

- Gehen Sie zu ***WAN PARTNER*** ➧ **ADD** ➧ ***PPP***.

Folgendes Menü öffnet sich:

```
X4x00 Setup Tool                              BinTec Access Networks GmbH
[WAN][ADD][PPP]: PPP Settings (BigBoss)                          MyRouter


    Authentication                CHAP + PAP
    Partner PPP ID                LittleIndian
    Local PPP ID                  BigBoss
    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	**X4100/200/300**s Kennung.
PPP Password	Paßwort.
Keepalives	Aktiviert Keepalive-Pakete zur Überprüfung der Erreichbarkeit der PPP-Gegenstelle. Mögliche Werte: ■ *off* ■ *on*
Link Quality Monitoring	Aktiviert PPP Link Quality Monitoring nach RFC 1989. Mögliche Werte: ■ *off* ■ *on* Nur notwendig in Ausnahmefällen, z. B. mit Nokia Communicator.

Tabelle 6-25: ***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.
MS-CHAP V2	Nur MS-CHAP Version 2 ausführen.
none	Kein PPP-Authentisierungsprotokoll ausführen.

Tabelle 6-26: **Authentication**

ToDo Nehmen Sie folgende Eintragungen vor:

- Wählen Sie **Authentication** aus, z. B. ***CHAP***.
- Geben Sie **Partner PPP ID** ein, z. B. ***LittleIndian***.
- Geben Sie **Local PPP ID** ein, z. B. ***BigBoss***.

Die Vorgehensweise bei der Eingabe von Paßwörtern ist unter Kapitel 4.4.4, Seite 71 beschrieben.

- 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 **X4100/200/300** nicht, welches Authentisierungsprotokoll mit diesem WAN-Partner festgelegt ist. Damit der Ruf trotzdem angenommen werden kann, greift **X4100/200/300** auf allgemeine Einstellungen im PPP zurück, die Sie nach Bedarf verändern können (siehe Kapitel 7.1.3, Seite 186).

Shorthold festlegen

Stellen Sie als nächstes Shorthold ein, um Gebühren zu sparen. **X4100/200/300** bricht dann die ISDN-Verbindung ab, wenn keine Daten mehr fließen. Mit statischem bzw. dynamischem Shorthold legen Sie fest, nach welchem Inaktivitätsintervall (Idle Timer) **X4100/200/300** die ISDN-Verbindung abbauen soll.

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

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

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

Grafische Darstellung Shorthold:

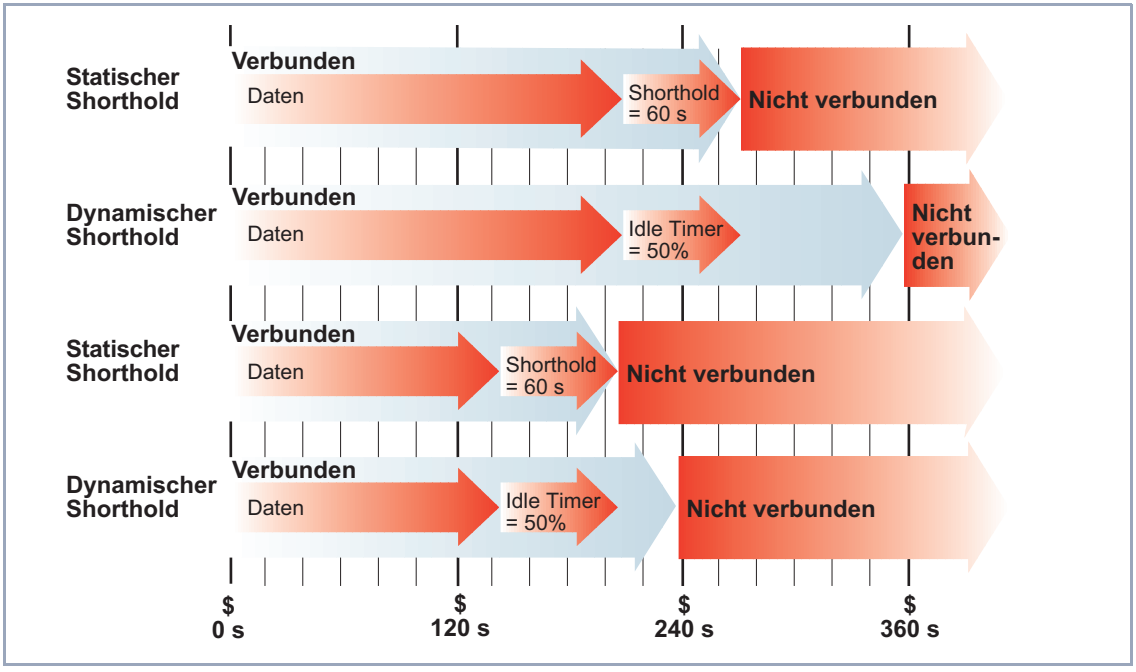


Bild 6-5: Dynamischer und statischer Shorthold

Bitte beachten Sie: dynamischen Shorthold können Sie nur nutzen, wenn Sie die Gebühreninformationen 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 Dauerwählverbindung zu haben.

Dabei sollten Sie darauf achten, daß der statische Shorthold später als der dynamische einsetzt. Andernfalls beendet **X4100/200/300** 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 zum Zeitpunkt der Drucklegung keine anderen Anbieter als die Deutsche Telekom Gebühreninformationen.

Gehen Sie folgendermaßen vor:

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

Folgendes Menü öffnet sich:

```
X4x00 Setup Tool                          BinTec Access Networks GmbH
[WAN][ADD][ADVANCED]: Advanced Settings (BigBoss)             MyRouter


Callback                                  no
Static Short Hold (sec)                   20
Idle for Dynamic Short Hold (%)           0
Delay after Connection Failure (sec)      300
Layer 1 Protocol                          ISDN 64 kbps

Channel-Bundling                          no



Extended Interface Settings (optional) >


                 OK                                    CANCEL

Use <Space> to select
```

Folgende Felder 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 Prozent für dynamischen Shorthold. Nur wirksam, wenn Gebühreninformationen während der Verbindung übermittelt werden (AOCD).

Tabelle 6-27: ***WAN PARTNER*** ➧ **ADD** ➧ ***ADVANCED SETTINGS***

ToDo Nehmen Sie folgende Eintragungen vor:

- 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***.

Folgendes Menü öffnet sich:

```
X4x00 Setup Tool                          BinTec Access Networks GmbH
[WAN][ADD][IP]: IP Configuration (BigBoss)                   MyRouter


    IP Transit Network                    no

    local IP Address

    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 **X4100/200/300** ein Transit Network zum WAN-Partner aufbaut.
local IP Address	IP-Adresse von **X4100/200/300**. Im Normalfall müssen Sie hier keinen Eintrag machen, außer Sie richten für einen Ihrer WAN-Partner ein Transitnetzwerk ein (siehe Kapitel 7.2.7, Seite 214).
local ISDN IP Address	ISDN-IP-Adresse von **X4100/200/300** im Transit Network.

Feld	Bedeutung
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 **X4100/200/300** eine Standard-Netzmaske für die unter *Partner's LAN IP Address* verwendete Netzklasse ein.

Tabelle 6-28: ***WAN PARTNER*** ➧ **ADD** ➧ ***IP***

ToDo Nehmen Sie folgende Eintragungen vor (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 **X4100/200/300** bekommt die **local ISDN IP Address** dynamisch (für die Dauer der Verbindung) oder statisch vom ISP zugewiesen. Nehmen Sie in diesem Fall folgende Einstellungen in ***WAN PARTNER*** ➧ **ADD** ➧ ***IP*** vor:

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: **X4100/200/300**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 **X4100/200/300**s statische IP-Adresse, die Sie vom ISP erhalten.
Keine Eintragungen für **Partner's LAN IP Address** und **Partner's LAN Netmask**.

Informationen zu Transit Network finden Sie in Kapitel 7.2.7, Seite 214.

Um den Domain-Name-Server des ISP während der Verbindung zu nutzen, nehmen Sie folgende Einstellungen vor 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.

6.3.2 Routing-Eintrag erstellen

Sie haben in Kapitel 6.3.1, Seite 148 einen WAN-Partner auf **X4100/200/300** eingerichtet. Für jeden WAN-Partner wird automatisch ein Routing-Eintrag in der Routing-Tabelle von **X4100/200/300** erzeugt. Die Routing-Einträge können Sie ändern und weitere hinzufügen. Für die Verbindung zu Ihrem Internet Service Provider sollten Sie immer eine sogenannte Default-Route einrichten.

In Menü ***IP*** ➧ ***ROUTING*** sind alle eingetragenen IP-Routen aufgelistet:

```
X4x00 Setup Tool                                BinTec Access Networks GmbH
[IP][ROUTING]: IP Routing                                         MyRouter

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

Destination  Gateway          Mask         Flags    Met  Interface    Pro
192.168.1.1  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             ADDEXT           DELETE              EXIT

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

Unter **Flags** wird der aktuelle Status (*Up* – Aktiv, *Dormant* – Ruhend, *Blocked* – Gesperrt) und die Art der Route (*Gateway Route*, *Interface Route*, *Subnet Route*, *Host Route*, *Extended Route*) angezeigt. Unter **Pro** wird angezeigt, mit welchem Protokoll **X4100/200/300** den Routing-Eintrag "gelernt" hat.

Route festlegen

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.

Um Einträge für Extended Routing (Erweitertes IP-Routing) zu erzeugen, betätigen Sie die Schaltfläche **ADDEXT** und öffnen damit das entsprechende Menü. Beachten Sie in dem Fall Kapitel 9.2.12, Seite 357.

Ein weiteres Menüfenster öffnet sich:

```
X4x00 Setup Tool                              BinTec Access Networks GmbH
[IP][ROUTING][ADD]: IP Routing                                   MyRouter


    Route Type                    Network route
    Network                       WAN without transit network

    Destination IP-Address        10.1.1.0
    Netmask                       255.255.255.0
    Partner / Interface           BigBoss

    Metric                        1


                SAVE                        CANCEL

Use <Space> to select
```

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), siehe Tabelle 6-30, Seite 168.
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 **X4100/200/300** die IP-Pakete weitergeben soll.

Feld	Bedeutung
Metric	Je niedriger der Wert, desto höhere Priorität besitzt die Route. (Wertebereich 1...14)

Tabelle 6-29: ***IP*** ➧ ***ROUTING*** ➧ **ADD**

Das Feld **Network** enthält folgende Auswahlmöglichkeiten:

Mögliche Werte	Bedeutung
LAN	Route zu einem Ziel-Host oder -LAN, das über **X4100/200/300**s LAN-Anschluß zu erreichen ist.
WAN without transit network	Route zu einem Ziel-Host oder -LAN, welche über einen WAN-Partner ohne Berücksichtigung eines evtl. vorhandenen Transitnetzwerks zu erreichen sind.
WAN with transit network	Route zu einem Ziel-Host oder -LAN, welche über einen WAN-Partner nur über ein Transitnetzwerk zu erreichen sind.
Refuse	**X4100/200/300** verwirft Datenpakete, die diese Route benutzen, und übermittelt dem Absender eine Meldung, daß das Ziel des Paketes unerreichbar ist.
Ignore	**X4100/200/300** verwirft Datenpakete, die diese Route benutzen, ohne eine Statusmeldung zu senden.

Tabelle 6-30: **Network**

Sie können auf **X4100/200/300** mehrere Default-Routen eintragen, aber nur eine einzige Default-Route kann jeweils wirksam sein. 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 z. B. eine Firmennetzanbindung machen, dann tragen Sie die Route zur Zentrale bzw. zur Filiale nur dann als Default-Route ein, wenn Sie keinen Internetzugang über **X4100/200/300** einrichten.
Wenn Sie z. B. sowohl einen Zugang zum Internet, als auch eine Firmennetzanbindung einrichten, dann tragen Sie zum ISP eine Default-Route und zur Firmenzentrale eine Netzwerk-Route ein.

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 temporär gespeichert und aktiviert. Die eingetragene oder geänderte Route ist aufgelistet.

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

Network Route Grafische Darstellung eines Netzwerkes mit Subnetzen:

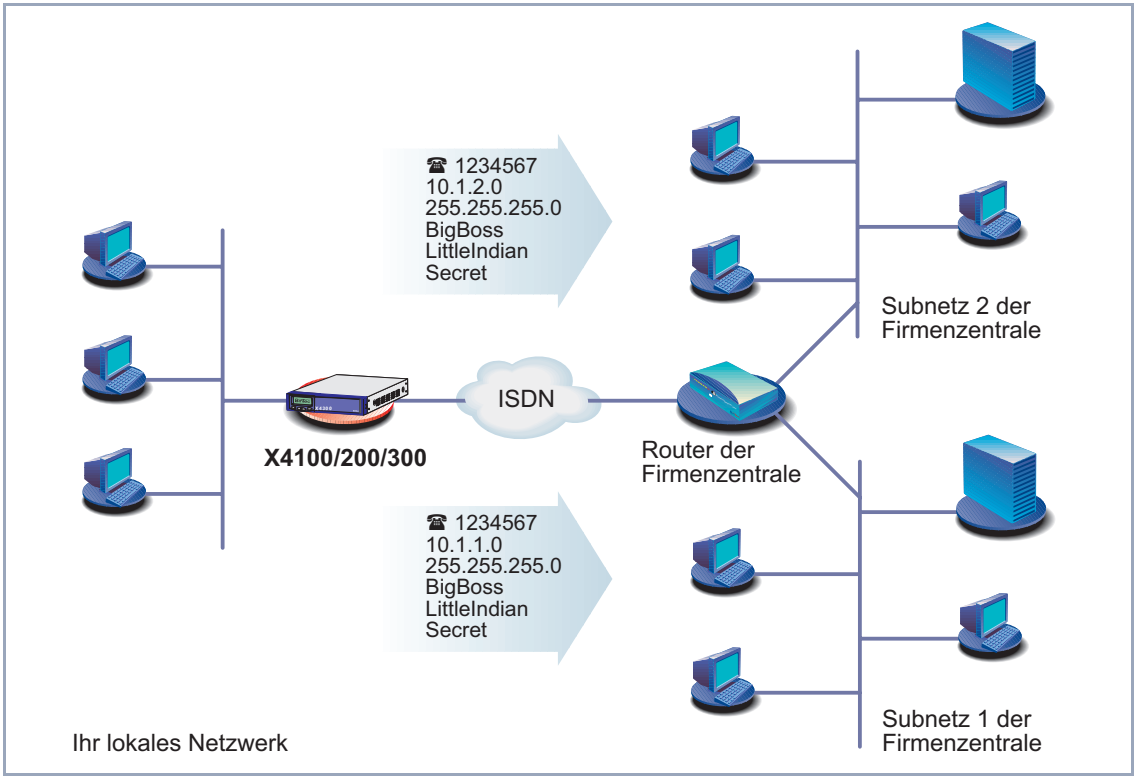


Bild 6-6: Netzwerk mit Subnetzen

Gehen Sie folgendermaßen vor, um eine Netzwerkroute, 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 temporär gespeichert und aktiviert. Die eingetragene oder geänderte Route ist aufgelistet.

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

6.3.3 Network Address Translation (NAT) aktivieren

Dieses Kapitel erläutert, wie Sie für Ihren WAN-Partner "Network Address Translation" (➤➤ **NAT**) 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 9.2.7, Seite 334.

NAT aktivieren

Gehen Sie folgendermaßen vor, um NAT zu aktivieren:

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

Folgendes Menü öffnet sich:

```
X4x00 Setup Tool                          BinTec Access Networks GmbH
[IP][NAT]: NAT Configuration                                  MyRouter

Select IP Interface to be configured for NAT

                     Nat          static mappings

GoInternet           on           2
LittleIndian         off
en1                  off
en1-snap             off


EXIT

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

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

Ein weiteres Menü öffnet sich:

```
X4x00 Setup Tool                          BinTec Access Networks GmbH
[IP][NAT][CONFIG]: NAT Configuration (GoInternet)            MyRouter

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 Nehmen Sie folgende Eintragungen vor:

- 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.

Bei aktiviertem NAT sind zunächst nur ausgehende Sessions zugelassen. Um bestimmte Verbindungen von außen zu Hosts innerhalb des LANs zu erlauben, müssen diese explizit definiert und zugelassen werden. Wie Sie dabei vorgehen, finden Sie in Kapitel 9.2.7, Seite 334.

6.3.4 Beispiele für WAN-Partner-Einstellungen

Im folgenden werden die WAN-Partner-Einstellungen für einige Beispielkonfigurationen angegeben:

- "Internetzugang über T-Online", Seite 173
- "Internetzugang über Compuserve", Seite 174

Die Vorgehensweise bei der Eingabe von Paßwörtern ist unter Kapitel 4.4.4, Seite 71 beschrieben.

Internetzugang über T-Online

T-Online

Folgende Einstellungen sind erforderlich:

- In ***WAN PARTNER*** ➧ **ADD**:
  Partner Name: *T_ONLINE*
  Encapsulation: *PPP*
  Compression: *none*
  Encryption: *none*

- In ***WAN PARTNER*** ➧ **ADD** ➧ ***WAN NUMBERS*** ➧ **ADD**:
  Number (= Einwahlnummer): z. B. ***0191011***
  Direction: *outgoing*

- In ***WAN PARTNER*** ➧ **ADD** ➧ ***PPP***:
  Authentication: *CHAP + PAP*
  Local PPP ID (= Anschlußkennung + T-Online-Nummer + Mitbenutzerkennung): z. B. ***123456789012081512345678#0001***
  PPP Password: z. B. ***mycat***
  Keepalives: *off*
  Link Quality Monitoring: *off*

- In ***WAN PARTNER*** ➧ **ADD** ➧ ***ADVANCED SETTINGS***:
  Callback: *no*
  Static Short Hold (sec): z. B. ***60***
  Idle for Dynamic Short Hold (%): z. B. ***0***
  Delay after Connection Failure (sec): z. B. ***300***
  Channel Bundling: *no*
  Layer 1 Protocol: *ISDN 64 kbps*

- In ***WAN PARTNER*** ➧ **ADD** ➧ ***IP***:
  IP Transit Network: *dynamic client*

- In ***WAN Partner*** ➧ **ADD** ➧ ***IP*** ➧ ***Advanced Settings***:
  RIP Send: *none*
  RIP Receive: *none*
  Van Jacobson Header Compression: *off*
  Dynamic Name Server Negotiation: *client (receive)*
  IP Accounting: *off*
  Back Route Verify: *off*
  Route Announce: *up or dormant*
  Proxy Arp: *off*

- In ***IP*** ➧ ***Routing*** ➧ **ADD**:
  Route Type: *Default route*
  Network: *WAN without transit network*
  Partner / Interface: *T_ONLINE*
  Metric: z. B. ***1***

- In ***IP*** ➧ ***Network Address Translation*** ➧ **T_Online** ➧ **Eingabetaste**:
  Network Address Translation: *on*

Internetzugang über Compuserve

Compuserve

Folgende Einstellungen sind erforderlich:

- In ***WAN Partner*** ➧ **ADD**:
  Partner Name: *COMPUSERVE*
  Encapsulation: *Async PPP over X.75*
  Compression: *none*
  Encryption: *none*

- In ***WAN Partner*** ➧ **ADD** ➧ ***WAN Numbers*** ➧ **ADD**:
  Number (= Einwahlnummer): z. B. ***010880191919***
  Direction: *outgoing*

- In ***WAN Partner*** ➧ **ADD** ➧ ***PPP***:
  Authentication: *none*
  Keepalives: *off*
  Link Quality Monitoring: *off*

- In ***WAN PARTNER*** ➧ **ADD** ➧ ***ADVANCED SETTINGS***:
  Callback: *no*
  Static Short Hold (sec): z. B. ***120***
  Idle for Dynamic Short Hold (%): z. B. ***0***
  Delay after Connection Failure (sec): z. B. ***300***
  Channel Bundling: *no*
  Layer 1 Protocol: *ISDN 64 kbps*

- In ***WAN PARTNER*** ➧ **ADD** ➧ ***ADVANCED SETTINGS*** ➧ ***COMPUSERVE LOGIN***:
  Provider: Compuserve Network
  Host: CIS
  User ID (= Ihr Benutzername)
  Password

- In ***WAN PARTNER*** ➧ **ADD** ➧ ***IP***:
  IP Transit Network: *dynamic client*

- In ***WAN PARTNER*** ➧ **ADD** ➧ ***IP*** ➧ ***ADVANCED SETTINGS***:
  RIP Send: *none*
  RIP Receive: *none*
  Van Jacobson Header Compression: *off*
  Dynamic Name Server Negotiation: *client (receive)*
  IP Accounting: *off*
  Back Route Verify: *off*
  Route Announce: *up or dormant*
  Proxy Arp: *off*

- In ***IP*** ➧ ***ROUTING*** ➧ **ADD**:
  Route Type: *Default route*
  Network: *WAN without transit network*
  Partner / Interface: *COMPUSERVE*
  Metric: z. B. ***1***

- In ***IP*** ➧ ***NETWORK ADDRESS TRANSLATION*** ➧ **COMPUSERVE** ➧ **EDIT**:
  Network Address Translation: *on*

6.4 Konfiguration sichern

Nachdem Sie nun eine Konfiguration auf **X4100/200/300** erstellt haben, sollten Sie diese sichern:

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

Ein weiteres Menüfenster öffnet sich:

```
X4x00 Setup Tool                              BinTec Access Networks GmbH
[EXIT]: Exit Setup                                                MyRouter


            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 öffnet sich die SNMP-Shell von **X4100/200/300** mit der Eingabeaufforderung. Alle Änderungen, die Sie vorher mit dem Setup Tool durchgeführt haben, sind im Flash gesichert. Beim nächsten Starten von **X4100/200/300** wird die so abgespeicherte Konfigurationsdatei geladen.
- Wählen Sie **Exit without saving**, um das Setup Tool zu verlassen, die vorgenommenen Änderungen aber nicht im Flash zu sichern.

  Es öffnet sich die SNMP-Shell von **X4100/200/300** mit der Eingabeaufforderung. Alle Änderungen, die Sie vorher mit dem Setup Tool durchgeführt haben, gehen beim Ausschalten von **X4100/200/300** verloren.

6.5 Kommunikationsanwendungen

Möchten Sie Kommunikationsanwendungen (CAPI) nutzen, sollten Sie jetzt die CAPI-Konfiguration durchführen. CAPI ermöglicht Ihnen u. a. das Versenden und Empfangen von Faxen und eine Anrufbeantworterfunktion.

Remote-CAPI konfigurieren

- Wählen Sie **Start** ➧ **Programme** ➧ **BRICKware** ➧ **CAPI and TAPI Configuration**.
- Tragen Sie im Register **Remote CAPI** die IP-Adresse von **X4100/200/300**, Benutzernamen und Paßwort der mit dem Setup Tool eingerichteten Nutzer der Kommunikationsanwendungen ein. Klicken Sie auf **Use these values**. Klicken Sie auf **OK**.

6.6 Konfiguration testen

Testen Sie nun, ob Sie alle Konfigurationseinstellungen richtig vorgenommen haben:

Achtung!

Durch eine Fehlkonfiguration der Geräte im LAN kann es zu ungewollten Verbindungen und erhöhten Gebühren kommen! Kontrollieren Sie, ob **X4100/200/300** Verbindungen nur zu gewollten Zeiten aufbaut!

- Um unnötige Gebühren zu vermeiden, prüfen Sie, ob die in Kapitel 6.1.5, Seite 115 eingestellten Filter für Ihre Bedürfnisse ausreichend sind. Sie können weitere Filter mit dem Setup Tool konfigurieren (Kapitel 9.2.8, Seite 339).
- Beobachten Sie die Leuchtanzeigen von **X4100/200/300** (vgl. Kapitel 3.5, Seite 49), benutzen Sie die Monitorfunktion des Setup Tools (vgl. Kapitel 9.1, Seite 312), fragen Sie Ihre Einstellungen am Display ab (vgl. Kapitel 5, Seite 83) oder prüfen Sie Ihre Einstellungen mit einem SNMP-Management-Tool.

LAN-Verbindung testen

Testen Sie die Verbindung zu **X4100/200/300**:

- Klicken Sie im Startmenü Ihres PCs auf **Ausführen** und geben Sie `ping` gefolgt von einem Leerzeichen und der IP-Adresse von **X4100/200/300** ein, z. B. `ping 192.168.1.254`. Bei korrekter Konfiguration öffnet sich ein Fenster mit dem Hinweis "`Antwort von 192.168.1.254...`".

Internetzugang testen

- Testen Sie den Internetzugang, indem Sie im Internet-Browser www.bintec.de eingeben.

  Bei korrekter Konfiguration öffnet sich BinTecs Startseite. Auf BinTecs Internetseiten finden Sie Neuigkeiten, Updates und weiterführende Dokumentation.

7 Weiterführende Konfiguration des Grundgeräts mit dem Setup Tool

In diesem Kapitel finden Sie weitere Möglichkeiten zur Konfiguration von **X4100/200/300** für den fortgeschrittenen Benutzer.

Folgende Konfigurationsschritte werden erläutert:

- Allgemeine ➤➤ **WAN**-Einstellungen (Kapitel 7.1, Seite 180)
- WAN-Partner-spezifische Einstellungen (Kapitel 7.2, Seite 190)
- Grundlegende ➤➤ **IP**-Einstellungen (Kapitel 7.3, Seite 233)
- "Quality of Service" (QoS) (Kapitel 7.4, Seite 260)
- Bridging (Kapitel 7.5, Seite 284)
- Funktionen mit Zusatzlizenz (Kapitel 7.6, Seite 285)

Nutzen Sie die Funktion Taschengeldkonto (siehe Kapitel 9.1.3, Seite 321). Damit können Sie für Verbindungen mit **X4100/200/300** ein Limit festlegen, um Gebühren aufgrund von Fehlern bei der Konfiguration einzuschränken.

7.1 Allgemeine WAN-Einstellungen

Dieses Kapitel beschreibt:

- **X4100/200/300** als dynamischer IP-Address-➤➤ **Server** (Kapitel 7.1.1, Seite 180)
- CAPI User Concept (Kapitel 7.1.2, Seite 182)
- Allgemeine ➤➤ **PPP**-Einstellungen (Kapitel 7.1.3, Seite 186)
- Einstellung des X.31-TEI-Werts (Kapitel 7.1.4, Seite 188)

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

7.1.1 Dynamic IP Address Server

IP-Address-Pools

X4100/200/300 kann als dynamischer IP-Address-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 einwählende WAN-Partner vergeben werden.

Eingetragene Host-Routen haben immer Vorrang vor IP-Adressen aus den Address-Pools. Wenn also ein eingehender Ruf authentisiert wurde, überprüft **X4100/200/300** zunächst, ob für den Anrufer in der Routing-Tabelle eine Host-Route eingetragen ist. Wenn dies nicht der Fall ist, kann **X4100/200/300** eine IP-Adresse aus einem Address-Pool zuweisen (falls verfügbar).

Bei Address-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 den Menüs ***IP*** ➧ ***IP ADDRESS POOL*** ***WAN (PPP)***, ***WAN PARTNER*** ➧ ***EDIT*** ➧ ***IP*** und ***WAN PARTNER*** ➧ ***EDIT*** ➧ ***IP*** ➧ ***ADVANCED SETTINGS***.

Menü ***IP*** ➧ ***IP ADDRESS POOL WAN (PPP)***:

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

Tabelle 7-1: ***IP*** ➧ ***IP ADDRESS POOL WAN (PPP)***

Menü ***WAN PARTNER*** ➧ ***EDIT*** ➧ ***IP***:

Feld	Bedeutung
IP Transit Network	Legt fest, ob zwischen **X4100/200/300** und WAN-Partner ein Transit-Netzwerk verwendet werden soll. Bei Zuweisung eines Address-Pools muß hier *dynamic server* ausgewählt werden.

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

Menü ***WAN PARTNER*** ➧ ***EDIT*** ➧ ***IP*** ➧ ***ADVANCED SETTINGS***:

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

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

ToDo Gehen Sie folgendermaßen vor, um **X4100/200/300** als dynamischen IP-Address-Server einzurichten:

➤ Gehen Sie zu ***IP*** ➧ ***IP ADDRESS POOL WAN (PPP)*** ➧ **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 Address-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**, bis Sie sich wieder im Hauptmenü befinden.

  Die Einstellungen sind temporär gespeichert und aktiviert. **X4100/200/300** ist als dynamischer IP-Address-Server eingerichtet.

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 Benutzername und Paßwort eingetragen sind, die CAPI-Dienste von **X4100/200/300** nutzen können.

Beispiel

Das CAPI User Concept ermöglicht, daß ein eingehendes Fax an den Benutzer ***Winnetou*** auch wirklich nur an den Benutzer ***Winnetou*** und nicht etwa an den Benutzer ***OldShatterhand***, der sich im gleichen LAN befindet, weitergeleitet wird. Wenn das CAPI User Concept nicht genutzt wird (siehe "Incoming Call Answering", Seite 125), 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.

Die Konfiguration erfolgt in den Menüs ***CAPI*** ➧ ***User*** und ***CM-1BRI, ISDN S0*** ➧ ***Incoming Call Answering***.

Menü ***CAPI*** ➧ ***USER***:

Feld	Bedeutung
Name	Benutzername, für den der 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 der 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***

Menü ***CM-1BRI, ISDN S0*** ➧ ***INCOMING CALL ANSWERING***:

Feld	Bedeutung
Item	Dienst, der einen Ruf auf die untenstehende **Number** annehmen soll.
Number	Rufnummer, unter welcher der oben eingetragene Dienst (**Item**) erreicht werden kann.
Mode	Modus, mit dem **X4100/200/300** den Ziffernvergleich von **Number** mit der Called Party's Number des eingehenden Rufes durchführt: *right to left:* Dies ist der Standard. *left to right (DDI):* Immer dann auswählen, wenn **X4100/200/300** mit einem Point-to-Point-Anschluß (Anlagenanschluß) verbunden ist.
Username	Entspricht **Name** in ***CAPI*** ➧ ***USER***. Benutzer, an den ein unter **Number** eingehender Ruf an den Dienst CAPI weitergeleitet werden soll.

Feld	Bedeutung
Bearer	Art des eingehenden Rufes. Mögliche Werte: ■ *data:* Datenruf ■ *voice:* Sprachruf (Modem, Sprache, analoges Fax) ■ *any:* beliebiger Ruf

Tabelle 7-5: ***CM-1BRI, ISDN S0*** ➧ ***INCOMING CALL ANSWERING***

Wenn sich beim Starten von **X4100/200/300** 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, um die Benutzer für den CAPI-Dienst einzutragen:

- 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.

Die Vorgehensweise bei der Eingabe von Paßwörtern im Setup Tool ist unter Kapitel 4.4.4, Seite 71 beschrieben.

- Wählen Sie **CAPI** aus.
- Bestätigen Sie mit **SAVE**.
- Wiederholen Sie diese Schritte für jeden CAPI-Benutzer im LAN.
- Gehen Sie zu ***CM-1BRI, ISDN S0*** ➧ ***INCOMING CALL ANSWERING***.

  Nehmen Sie hier für jeden Benutzer im LAN, der Zugriff auf den Dienst CAPI hat, einen Eintrag vor.

- 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 **X4100/200/300** die ➤➤ **MSN** (=**Number**, mehrstellig) des eingehenden Rufes in ➤➤ **EAZ** (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, jeder CAPI-Anwendung die passende(n) EAZ(s) per "mapping" zuzuteilen. Wählen Sie 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.

Sie sollten auf jeden Fall versuchen, Ihr Rechnersystem auf CAPI 2.0 umzustellen, um auch neue Leistungsmerkmale nutzen zu können.

- Geben Sie **Number** ein.
- Wählen Sie **Mode** aus.
- Geben Sie **Username** ein.
- Wählen Sie **Bearer** aus.
- Bestätigen Sie mit **SAVE**.
- Wiederholen Sie diese Schritte, bis Sie für jeden CAPI-Benutzer einen CAPI-Eintrag erstellt haben.

Bei der Remote-CAPI-Konfiguration auf den Hosts müssen Sie dann für jeden Benutzer jeweils Benutzername und Paßwort eintragen, entsprechend den Eintragungen auf **X4100/200/300**.

7.1.3 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 6.3, Seite 147). Wenn ein Ruf eingeht, erkennt **X4100/200/300** 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 erfolgreich ist, wird der Ruf angenommen.

CLID

In folgenden Fällen kann ein eingehender Ruf nicht via CLID identifiziert werden:

- Der Ruf erfolgt über eine analoge Leitung (der Anrufer wählt sich per ➤➤ **Modem** auf Ihrem Router ein)
- Der Anrufer unterdrückt das Übermitteln der eigenen Rufnummer

In beiden Fällen kommt bei **X4100/200/300** keine Calling Line Number an. Eine Identifizierung des Anrufers via CLID kann also nicht erfolgen, auch wenn der Anrufer als WAN-Partner eingetragen ist. **X4100/200/300** weiß nicht, mit welchem ➤➤ **PPP-Authentisierung**sprotokoll er den eingehenden Ruf identifizieren kann.

Allgemeine PPP-Einstellungen

Um eine Rufannahme trotzdem zu ermöglichen, führt **X4100/200/300** mit dem Anrufer dasjenige 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 (Paßwort, Partner PPP ID) mit den Daten eines eingetragenen WAN-Partners übereinstimmen, akzeptiert **X4100/200/300** den ankommenden Ruf.

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 Anrufer gewollte Protokoll ■ *MS-CHAP V2*: nur MS-CHAP Version 2 ■ *none:* keine PPP-Authentisierung
Radius Server Authentication	Einstellungen zur RADIUS Server Authentisierung. Zu RADIUS siehe **Software Reference**.
PPP Link Quality Monitoring	Definiert, ob Link Quality Monitoring für PPP-Verbindungen durchgeführt wird (nur notwendig in Ausnahmefällen, z. B. mit Nokia Communicator). Mögliche Werte: ■ *no*, wird nicht durchgeführt. ■ *yes*, die Verbindungsstatistiken werden in der ➤➤ **MIB**-Tabelle **biboPPPLQMTable** gespeichert.
PPPoE Ethernet Interface	Definiert das Interface, über welches PPP-over-Ethernet zur Nutzung eines ADSL-Anschlusses läuft (siehe Kapitel 6.2.3, Seite 138).

Tabelle 7-6: ***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***.
- Bestätigen Sie mit **SAVE**.

  Die PPP-Einstellungen sind festgelegt.

7.1.4 X.31 TEI (Terminal Endpoint Identifier)

Im Menü ***CM-1BRI, ISDN S0*** ➧ ***ADVANCED SETTINGS*** finden Sie Einstellungen für X.31 (X.25 im D-Kanal). Sie müssen hier nur Änderungen vornehmen, wenn Sie den X.31-TEI-Wert z. B. für CAPI-Applikationen nutzen wollen.

Das Menü enthält folgende Felder:

Feld	Bedeutung
X.31 TEI Value	Bei ISDN-Autokonfiguration wird der X.31-TEI automatisch erkannt und dieser Wert auf *specify* gesetzt. Hat die Autokonfiguration den TEI nicht erkannt, können Sie hier manuell *specify* einstellen.
Specify TEI Value	Der Wert für den X.31-TEI, der von der Vermittlungsstelle zugewiesen wurde. Dieser Wert wird von der ISDN-Autokonfiguration automatisch erkannt, kann aber auch manuell eingegeben werden.

Feld	Bedeutung
X.31 TEI Service	Hier wählen Sie den Service, für den Sie den X.31-TEI nutzen wollen. Mögliche Werte: ■ *Capi* ■ *Capi Default* ■ *Packet Switch* *Capi* und *Capi Default* dienen zur Nutzung des X.31-TEI für CAPI-Applikationen. Bei *CAPI* wird der in der CAPI-Applikation eingestellte TEI-Wert benutzt, bei *Capi Default* wird der Wert der CAPI-Applikation ignoriert und immer der hier eingestellte Standardwert benutzt. *Packet Switch* stellen Sie ein, wenn Sie den X.31-TEI für den X.25-Router nutzen möchten.

Tabelle 7-7: ***CM-1BRI, ISDN S0*** ➧ ***ADVANCED SETTINGS***

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 (Kapitel 7.2.1, Seite 190)
- Channel Bundling (Kapitel 7.2.2, Seite 191)
- Bandwidth on Demand (BoD) (Kapitel 7.2.3, Seite 193)
- Always On/Dynamic ISDN (AO/DI) (Kapitel 7.2.4, Seite 198)
- Applikationsgesteuertes Bandbreitenmanagement (Kapitel 7.2.5, Seite 206)
- Layer 1 Protocol (ISDN-B-Kanal) (Kapitel 7.2.6, Seite 211)
- IP Transit Network (Kapitel 7.2.7, Seite 214)
- Übermittlung von DNS- und WINS-Server-IP-Adressen an WAN-Partner (Kapitel 7.2.8, Seite 217)
- ➤➤ **RIP** (Routing Information Protocol) (Kapitel 7.2.9, Seite 220)
- Komprimierung: ➤➤ **VJHC**, ➤➤ **STAC**, MS-STAC (Kapitel 7.2.10, Seite 222)
- ➤➤ **Proxy ARP** (Address Resolution Protocol) (Kapitel 7.2.11, Seite 224)
- Keepalive Monitoring (Kapitel 7.2.12, Seite 227)

Im folgenden werden die jeweils erforderlichen Konfigurationsschritte genau erläutert.

7.2.1 Delay after Connection Failure

Mit dieser Funktion richten Sie eine Wartezeit nach fehlgeschlagenem Verbindungsversuch durch **X4100/200/300** 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 fehlgeschlagenen Verbindungsaufbau kein erneuter Versuch durch **X4100/200/300** unternommen wird.

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**.
  Die Wartezeit ist eingetragen.

7.2.2 Channel Bundling

X4100/200/300 unterstützt dynamische und statische ➤➤ **Kanalbündelung** für Wählverbindungen. Bei Aufbau einer Verbindung wird zunächst nur ein B-Kanal geöffnet.

Dynamisch Dynamische Kanalbündelung bedeutet, daß **X4100/200/300** bei Bedarf, also bei großen Datenmengen, weitere ➤➤ **ISDN**-B-Kanäle für Verbindungen mit dem WAN-Partner zuschaltet, um den Durchsatz zu erhöhen. Sinkt das Datenaufkommen, werden die zusätzlichen ➤➤ **B-Kanäle** wieder geschlossen.

Statisch Bei statischer Kanalbündelung legen Sie von vorneherein fest, wie viele B-Kanäle **X4100/200/300** für Verbindungen mit dem WAN-Partner nutzen soll, unabhängig von der übertragenen Datenmenge.

Die Konfiguration erfolgt in ***WAN PARTNER*** ➧ ***EDIT*** ➧ ***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 gesamten Verbindungsdauer geöffnet sind.

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**.
  Die Einstellungen sind eingetragen.

Beachten Sie auch die Funktion "Bandwidth on Demand" (BOD), siehe Kapitel 7.2.3, Seite 193.

7.2.3 Bandwidth on Demand (BOD)

Mit dieser Funktion ist das dynamische Bündeln von Festverbindungen mit Wählverbindungen aufgrund von hohem Datenfluß möglich. Sie haben die folgenden Optionen:

- BOD für Festverbindungen, d. h. dynamisches Zuschalten von einer oder mehreren Wählverbindung(en) zur bestehenden Festverbindung bei Bedarf.
- BOD für Wählverbindungen, d. h. dynamisches Zuschalten von einer oder mehreren Wählverbindung(en) zur bestehenden Wählverbindung bei Bedarf.
- Backup für Festverbindungen, d. h. Aufbauen einer Wählverbindung, wenn die Festverbindung zum Partner ausfällt. Auch bei ausgefallener Festverbindung greift BOD (d. h. können weitere Wählverbindungen zugeschaltet werden), falls bei der Konfiguration mehr als ein zusätzlicher Kanal erlaubt wurde (**Maximum Number of Dialup Channels** > *1*).

Zu- und Abschalten von B-Kanälen

Die Verwendung der B-Kanäle wird anhand des Datendurchsatzes oder über applikationsabhängiges Bandbreitenmanagement (Bandwidth on Demand, BOD für IP-basierende Applikationen) geregelt.

Einerseits können B-Kanäle zugeschaltet werden, sobald die Bandbreite des D-Kanals für eine Datenübertragung nicht mehr ausreicht. Die Datenübertragung erfolgt dann ausschließlich in den B-Kanälen (Dynamic ISDN). Ein B-Kanal wird zugeschaltet, wenn die aktuelle Auslastung der entsprechenden Schnittstelle zum Verbindungspartner für mindestens fünf Sekunden 90% oder mehr der maximal möglichen Auslastung beträgt. Aus der gemessenen Auslastung wird die prozentuale Auslastung des Bündels unter Annahme eines abgeschalteten B-Kanals berechnet. Ein B-Kanal wird abgeschaltet, wenn der berechnete Wert zehn Sekunden lang unter 80% der maximal möglichen Auslastung der übrigbleibenden Kanäle bleibt.

Andererseits ist die applikationsgesteuerte Zuschaltung von B-Kanälen **X4100/200/300** über Filter und Regeln in ähnlicher Weise konfigurierbar wie Access-Listen für IP-Pakete. Konfigurationserläuterungen dazu finden Sie in Kapitel 7.2.5, Seite 206.

Sowohl das durchsatzabhängige als auch das applikationsgesteuerte Bandbreitenmanagement nutzt das "Bandwidth Allocation Control Protocol" (BACP/BAP nach RFC 2125), um mit der Gegenstelle zu vereinbaren, unter welchen Umständen B-Kanäle zu- bzw. abgeschaltet werden sollen. Die Verwendung von BACP/BAP wird während des initialen Verbindungsaufbaus vereinbart.

Statischer oder dynamischer Shorthold (siehe "Shorthold festlegen", Seite 159) können ebenso zum Abschalten eines zusätzlichen B-Kanals führen. Wenn statischer Shorthold konfiguriert wurde, hat dieser immer die höchste Priorität. Wenn dynamischer Shorthold konfiguriert wurde, muß zusätzlich der oben genannte berechnete Wert zutreffen.

X4100/200/300 unterstützt auch die Funktion AO/DI (Always On/Dynamic ISDN), um den ISDN-D-Kanal zur Datenübertragung zu nutzen (siehe Kapitel 7.2.4, Seite 198).

Authentisierung

Für das Aufbauen einer Festverbindung ist keine PPP-Authentisierung der Verbindungspartner erforderlich. Dagegen ist eine Authentisierung für die gegebenenfalls zugeschalteten Wählverbindungen nötig.

Die Konfiguration erfolgt in:

- ***WAN PARTNER*** ➧ ***EDIT*** ➧ ***ADVANCED SETTINGS*** ➧ ***EXTENDED INTERFACE SETTINGS (OPTIONAL)***
- ***WAN PARTNER*** ➧ ***EDIT*** ➧ ***WAN NUMBERS*** ➧ **ADD** (Beschreibung des Menüs in Kapitel 6.2, Seite 121)
- ***WAN PARTNER*** ➧ ***EDIT*** ➧ ***PPP*** (Beschreibung des Menüs in Kapitel 6.3, Seite 147)

Die im folgenden beschriebenen Felder erscheinen nur, wenn vorher im Menü ***WAN PARTNER*** ➧ ***EDIT*** ➧ ***ADVANCED SETTINGS*** unter **Channel Bundling** = *dynamic* ausgewählt wurde.

Das Menü ***WAN Partner*** ➧ ***Edit*** ➧ ***Advanced Settings*** ➧ ***Extended Interface Settings (optional)*** enthält folgende Felder:

Feld	Bedeutung
Mode	Legt fest, welcher Modus für BOD verwendet wird. Mögliche Werte: siehe Tabelle 7-12, Seite 197.
Line Utilization Weighting	Legt fest, wie die Auslastung der Verbindung berechnet wird. Mögliche Werte: ■ *equal:* Für die Berechnung werden alle gemessenen Werte für den Durchsatz innerhalb von **Line Utilization Sample (sec)** gleich gewichtet (Standardwert). ■ *proportional:* Für die Berechnung werden die zuletzt gemessenen Werte für den Durchsatz stärker gewichtet. D. h. die Berechnung wird am stärksten von den innerhalb von **Line Utilization Sample (sec)** zuletzt gemessenen Werten beeinflußt.
Line Utilization Sample (sec)	Zeitintervall in Sekunden. Durchsatzmessungen innerhalb von **Line Utilization Sample (sec)** gehen in die Berechnung der Auslastung einer Verbindung ein. Mögliche Werte: *5* bis *300* (Standardwert: *5*).
Gear Up Threshold	Auslastung, ab der bei einer Verbindung ein weiterer B-Kanal zugeschaltet wird.
Gear Down Threshold	B-Kanäle werden weggeschaltet, bis die verbleibenden Kanäle mindestens den hier verbleibenden Auslastungsgrad in Prozent aufweisen.

Feld	Bedeutung
D-Channel Queue Length	(nur bei **Layer 1 Protocol** = *AO/DI* im Menü ***WAN Partner*** ➧ ***Edit*** ➧ ***Advanced Settings***) Schwellwert für die im D-Kanal angesammelte Anzahl von Bytes, ab der in den B-Kanal-Modus gewechselt werden soll (siehe Kapitel 7.2.4, Seite 198).
Maximum Number of Dialup Channels	Maximal erlaubte Anzahl der Kanäle, die für Wählverbindungen geöffnet werden. Der Wert wird an dieser Stelle nur angezeigt, eingestellt wird er im Menü ***WAN Partner*** ➧ ***Edit*** ➧ ***Advanced Settings*** unter **Total Number of Channels**.

Tabelle 7-11: ***WAN Partner*** ➧ ***Edit*** ➧ ***Advanced Settings*** ➧ ***Extended Interface Settings (optional)***

Das Feld **Mode** enthält folgende Auswahlmöglichkeiten:

Mögliche Werte	Bedeutung
Bandwidth On Demand Disabled	Deaktiviert BOD, es werden keine zusätzlichen Kanäle geöffnet (Standardwert).
Bandwidth On Demand Enabled	(Nur bei Wählverbindungen) Aktiviert BOD, es können zusätzliche Kanäle geöffnet werden. Der Verbindungspartner, der die Verbindung initiiert hat, öffnet die zusätzlichen Kanäle.
BAP, Active Mode	(Bandwidth Allocation Protocol) Erforderlich für die Funktion AO/DI (Always On/Dynamic ISDN), siehe Tabelle 7-17, Seite 205
BAP, Passive Mode	Wird derzeit von **X4100/200/300** nicht unterstützt.
BAP, Active and Passive Mode	Wird derzeit von **X4100/200/300** nicht unterstützt.

Mögliche Werte	Bedeutung
BAP, Client Active Mode	Wird derzeit von **X4100/200/300** nicht unterstützt.
Backup	(Nur bei Festverbindungen) Die Backup-Verbindung wird aktiviert, falls die Festverbindung ausfällt. Wenn die Festverbindung wieder verfügbar ist, wird die Backup-Verbindung abgebaut. BOD ist auch für diesen Modus verfügbar, falls für **Maximum Number of Dialup Channels** ein Wert > 1 verwendet wird.
Bandwidth On Demand Active	(Nur bei Festverbindungen) Ermöglicht BOD und definiert den aktiven Partner. Nur einer der Verbindungspartner sollte als aktiver Partner konfiguriert sein. Diese Seite aktiviert dann bei Bedarf das Zu- und Abschalten von zusätzlichen B-Kanälen.
Bandwidth On Demand Passive	(Nur bei Festverbindungen) Ermöglicht BOD und definiert den passiven Partner. Diese Seite aktiviert kein Zu- und Abschalten von zusätzlichen Kanälen.

Tabelle 7-12: **Mode**

ToDo Gehen Sie folgendermaßen vor:

- Gehen Sie zu ***WAN PARTNER*** ➧ ***EDIT*** ➧ ***ADVANCED SETTINGS*** ➧ ***EXTENDED INTERFACE SETTINGS (OPTIONAL)***.
- Wählen Sie den gewünschten Wert für **Mode** und **Line Utilization Weighting** aus.
- Tragen Sie den gewünschten Wert für **Line Utilization Sample (sec)** ein.
- Bestätigen Sie mit **SAVE**.
- Bestätigen Sie mit **OK**.
- Gehen Sie zu ***WAN PARTNER*** ➧ ***EDIT*** ➧ ***WAN NUMBERS*** ➧ **ADD**.

- Tragen Sie **Number** ein.
- Wählen Sie **Direction** aus.

Wählen Sie **Direction** = *outgoing*, wenn Sie **Mode** = *Bandwidth On Demand Active* eingestellt haben.

Wählen Sie **Direction** = *incoming (CLID),* wenn Sie **Mode** = *Bandwidth On Demand Passive* eingestellt haben.

- Bestätigen Sie mit **SAVE**.
- Gehen Sie zu ***WAN PARTNER*** ➧ ***EDIT*** ➧ ***PPP***.
- Wählen Sie **Authentication** aus.
- Tragen Sie gegebenenfalls **Partner PPP ID**, **Local PPP ID** und **PPP Password** ein.
- Bestätigen Sie mit **OK**.
- Bestätigen Sie mit **SAVE**.

  Die Einstellungen sind konfiguriert.

7.2.4 Always On/Dynamic ISDN (AO/DI)

Always On/Dynamic ISDN (AO/DI) nutzt die bereits vorhandene ISDN-Infrastruktur, um ohne Hardware-Änderungen einen neuen Dienst für den Nutzer einzurichten: AO/DI stellt eine ständig verfügbare (always on) aber dennoch kostengünstige Verbindung vom Endkunden zum Service Provider dar. Zum Zeitpunkt der Drucklegung stellt dies nur die Deutsche Telekom zur Verfügung.

Kurzbeschreibung

AO/DI nutzt die X.25-Datenpaketübertragung im D-Kanal (X.31), um eine PPP-Verbindung (PPP over X.25) aufzubauen. Im D-Kanal stehen für die Datenübertragung 9600 Bit/s zur Verfügung (D-Kanal-Modus). Bei steigendem Bandbreitenbedarf werden ein oder mehr B-Kanäle dynamisch hinzugeschaltet (Dynamic ISDN). Die Datenübertragung erfolgt in diesem Fall ausschließlich im B-Kanal bzw. in den B-Kanälen (B-Kanal-Modus).

AO/DI bietet folgende Vorteile:

- Drei vollwertige, bei Bedarf unabhängige Kommunikationskanäle

- Permanenter Anschluß an das Internet zu wirtschaftlich günstigen Bedingungen
- Transparente Bandbreitenregelung
- Im D-Kanal-Modus
  - hohe Zuverlässigkeit und garantierte Durchlaufzeiten
  - volumenorientierter, entfernungsunabhängiger Tarif
- Im B-Kanal-Modus zeitabhängige Verbindungsgebühren nur für bandbreitenintensive Anwendungen

Wie funktioniert AO/DI?

AO/DI wird bei **X4100/200/300** über ein spezielles PPP-Interface realisiert. Sobald das Interface konfiguriert und betriebsbereit ist, erfolgt der initiale PPP-Verbindungsaufbau über X.31 (X.25 im D-Kanal). Dabei wird die Authentisierung des PPP-Verbindungspartners durchgeführt und gegebenenfalls eine dynamische IP-Adresse und DNS-Adressen zugewiesen (AO/DI-Client-Modus).

Da die D-Kanal-Verbindung normalerweise nach dem Verbindungsaufbau nicht mehr beendet wird, stellt sie eine ständig verfügbare (always on) Anbindung zum Provider dar.

Sobald die Bandbreite des D-Kanals für eine Datenübertragung nicht mehr ausreicht, werden B-Kanäle zugeschaltet und die Datenübertragung erfolgt ausschließlich in den B-Kanälen (Dynamic ISDN). Auf **X4100/200/300** ist dies durch eine erweiterte Konfigurationsmöglichkeit innerhalb des IP-Subsystems realisiert. Wie bei dem Konzept für IP-Access-Listen werden einem Interface Filter, Regeln und Regelketten zugewiesen (siehe Kapitel 9.2.8, Seite 339). Mit Hilfe dieser Regeln kann man festlegen, ob bei bestimmten Protokollen, Ports oder IP-Adressen zusätzliche B-Kanäle aufgebaut werden sollen oder ob der Datentransfer ausschließlich im D-Kanal erfolgen darf.

Wie wird AO/DI konfiguriert?

Um **X4100/200/300** für AO/DI zu konfigurieren, sind folgende Schritte erforderlich:

- X.31-Konfiguration durchführen, d. h. **TEI Value** für X.25 (Packet Switch) reservieren (siehe "X.31-Konfiguration", Seite 200)
- X.25 Konfiguration durchführen (siehe "X.25-Konfiguration", Seite 201):
  - Link-Konfiguration für Datex-P
  - Call-Routing
- AO/DI-Partner als WAN-Partner anlegen (siehe "AO/DI-Partner als WAN-Partner anlegen", Seite 202)
  - PPP-Parameter festlegen
  - das PPP-Interface als AO/DI-Interface definieren
  - X.25-Zieladresse für initialen Verbindungsaufbau eintragen
  - durchsatzabhängiges Bandbreitenmanagement (dynamische B-Kanalbündelung) regeln
  - applikationsabhängiges Bandbreitenmanagement regeln

Im folgenden finden Sie alle notwendigen Schritte, um **X4100/200/300** mit dem Setup Tool für AO/DI zu konfigurieren.

X.31-Konfiguration

Gehen Sie folgendermaßen vor, um X.31 X.25 zuzuordnen:

➤ Gehen Sie zu ***CM-1BRI, ISDN S0*** ➧ ***ADVANCED SETTINGS*** (das Menü ist beschrieben in Kapitel 7.1.4, Seite 188).

➤ Wählen Sie **X.31 TEI Value** aus: *specify*.

Für **X.31 TEI Value** sollte der voreingestellte Wert *specify* sein. Ist dies nicht der Fall, dann wurde der X.31-Dienst von der Autokonfiguration nicht erkannt, der X.31-Dienst wird in diesem Fall vermutlich nicht unterstützt (wenden Sie sich an Ihre Telefongesellschaft).

➤ Geben Sie **Specify TEI Value** ein, z. B. ***1***.

➤ Wählen Sie **X.31 TEI Service** aus: *Packet Switch*.

➤ Bestätigen Sie mit **SAVE**.

Sie befinden sich wieder im Menü ***CM-1BRI, ISDN S0***.

➤ Bestätigen Sie mit **SAVE**.

Sie befinden sich wieder im Hauptmenü. Das Hauptmenü enthält ab diesem Zeitpunkt das X.25-Menü, das für die folgenden Konfigurationsschritte benötigt wird. Informationen zu den X.25-Parametern finden Sie in der **Software Reference**.

X.25-Konfiguration

Bei der X.25-Konfiguration ist folgendes zu beachten:

- Einige der X.25-Parameter müssen dem angeschlossenen X.25-Netz angepaßt werden. Für Datex-P muß im Setup Tool die **Windowsize/ Packetsize Neg.** ausgeschaltet werden.
- Bei **X4100/200/300** ist die X.25-Software grundsätzlich als X.25-Switch ausgelegt. Für AO/DI muß dieser Switch entsprechend konfiguriert werden.

Um die Link-Voreinstellungen der X.25-Konfiguration für Datex-P vorzunehmen, gehen Sie folgendermaßen vor:

➤ Gehen Sie zu ***X.25*** ➧ ***LINK CONFIGURATION***.

➤ Wählen Sie die Schnittstelle aus, für die Sie X.25 konfigurieren möchten, z. B. ***x31d2-0-1***.

Folgende Felder des Menüs sind für diesen Konfigurationsschritt relevant:

Feld	Bedeutung
L3 Packet Size	Zulässige Größe der Datenpakete für diese Verbindung auf der dritten Ebene des OSI-Modells.
Windowsize/Packetsize Neg.	Aushandlung der Größe von **Windowsize** und **Packetsize** mit der Gegenseite. Für Datex-P gibt es nur eine sinnvolle Einstellung: *never*, d. h. die Aushandlung wird abgeschaltet.
Highest Two-Way-Channel (HTC)	Definiert die höchste Anzahl an zuschaltbaren virtuellen Kanälen.

Tabelle 7-13: ***X.25*** ➧ ***LINK CONFIGURATION*** ➧ ***EDIT***

➤ Wählen Sie **L3 Packet Size max** aus: *256*.

- Wählen Sie **Windowsize/Packetsize Neg.** aus: *never*.
- Geben Sie **Highest Two-Way-Channel (HTC)** ein: *1*.
- Bestätigen Sie mit **SAVE**.
- Verlassen Sie ***X.25*** ➧ ***LINK CONFIGURATION*** mit **Exit**.

Um die Routing-Voreinstellungen der X.25-Konfiguration vorzunehmen, gehen Sie folgendermaßen vor:

- Gehen Sie zu ***X.25*** ➧ ***ROUTING*** ➧ ***ADD***.

Folgende Felder des Menüs sind für diesen Konfigurationsschritt relevant:

Feld	Bedeutung
Source Link	Quellschnittstelle der Datenpakete.
Destination Link	Zielschnittstelle der Datenpakete.
Destination X.25 Address	X.25-Zieladresse

Tabelle 7-14: ***X.25*** ➧ ***ROUTING*** ➧ ***ADD***

- Wählen Sie **Source Link** aus: *local*.
- Wählen Sie **Destination Link** aus, z. B. ***x31d2-0-1***.
- Geben Sie **Destination X.25 Address** ein, z. B. ***019011***.
- Bestätigen Sie mit **SAVE**.
- Verlassen Sie ***X.25*** ➧ ***ROUTING*** ➧ ***ADD*** mit **Exit**.
- Verlassen Sie ***X.25*** ➧ ***ROUTING*** mit **Exit**.
  Sie befinden sich wieder im Hauptmenü.

AO/DI-Partner als WAN-Partner anlegen

Um ein AO/DI-fähiges PPP-Interface zu definieren, gehen Sie folgendermaßen vor:

- Gehen Sie zu ***WAN PARTNER*** ➧ ***ADD***.
- Geben Sie **Partner Name** ein, z. B. ***AODI-partner***.
- Wählen Sie **Encapsulation** aus: *PPP*.

Um die PPP-Einstellungen vorzunehmen, gehen Sie folgendermaßen vor:

- Gehen Sie zu ***WAN Partner*** ➧ ***ADD*** ➧ ***PPP***.
- Wählen Sie **Authentication** aus, z. B. ***CHAP***.
- Überspringen Sie **Partner PPP ID**.
- Geben Sie **Local PPP ID** ein, z. B. ***bintec_router***.
- Geben Sie zweimal **PPP Password** ein, z. B. ***secret***.

  Bei Eingabe des Paßworts erscheint auf dem Bildschirm für jeden Buchstaben ein Sternchen als Platzhalter.
- Bestätigen Sie mit **OK**.

Um AO/DI auf dem PPP-Interface zu aktivieren und die X.25-Adresse einzutragen, gehen Sie folgendermaßen vor:

- Gehen Sie zu ***WAN Partner*** ➧ ***ADD*** ➧ ***Advanced Settings***.

Folgende Felder des Menüs sind für diesen Konfigurationsschritt relevant:

Feld	Bedeutung
Layer 1 Protocol	Legt fest, welches Layer 1 Protocol **X4100/200/300** nutzen soll. Für AO/DI gibt es nur eine sinnvolle Einstellung: *AO/DI*.
Channel Bundling	Legt fest, ob bzw. welche Art von Kanalbündelung für Verbindungen mit dem WAN-Partner genutzt werden soll (siehe Kapitel 7.2.2, Seite 191) Wenn unter **Layer 1 Protocol** *AO/DI* ausgewählt ist, ist für **Channel Bundling** automatisch *dynamic* eingestellt.
Total Number of Channels	Definiert bei dynamischer Kanalbündelung die maximale Anzahl der B-Kanäle, die geöffnet sein dürfen.
Remote X.25 Address	X.25-Zieladresse. Erscheint nur, wenn unter **Layer 1 Protocol** *AO/DI* ausgewählt ist.

Tabelle 7-15: ***WAN Partner*** ➧ ***Add*** ➧ ***Advanced Settings***

- Wählen Sie **Layer 1 Protocol** aus: *AO/DI*.

- Geben Sie **Total Number of Channels** ein, z. B. ***2***.
- Geben Sie **Remote X.25 Address** ein, z. B. ***019011***.

Gehen Sie folgendermaßen vor, um BACP/BAP für den "AO/DI-Client"-Zugang zu konfigurieren (Regelung des durchsatzgesteuerten Bandbreitenmanagements):

- Gehen Sie zu ***WAN Partner*** ➧ ***add*** ➧ ***Advanced Settings*** ➧ ***extended Interface Settings (optional)***.

Folgende Felder des Menüs sind für diesen Konfigurationsschritt relevant:

Feld	Bedeutung
Mode	Legt fest, welcher Modus für BOD verwendet wird. Für AO/DI-Client wird ausschließlich die Einstellung *BAP, Active Mode* benutzt.
Line Utilization Weighting	Gewichtung innerhalb des Intervalls, das für die Zu- bzw. Abschaltung von B-Kanälen betrachtet wird.
Line Utilization Sample (sec)	Länge des Intervalls, über welches die gemessenen Durchsatzdaten gemittelt und mit **Line Utilization Weighting** gewichtet werden.
Gear Up Threshold	Auslastung, ab der bei einer Verbindung ein weiterer B-Kanal zugeschaltet wird.
Gear Down Threshold	B-Kanäle werden weggeschaltet, bis die verbleibenden Kanäle mindestens den hier verbleibenden Auslastungsgrad in Prozent aufweisen.
D-Channel Queue Length	Schwellwert für die im D-Kanal angesammelte Anzahl von Bytes, ab der in den B-Kanal-Modus gewechselt werden soll.
Maximum Number of Dialup Channels	Maximale Anzahl der Kanäle, die geöffnet werden dürfen. Der Wert wird unter ***WAN Partner*** ➧ ***add*** ➧ ***Advanced Settings*** im Feld **Total Number of Channels** festgelegt.

Tabelle 7-16: ***WAN Partner*** ➧ ***add*** ➧ ***Advanced Settings*** ➧ ***extended Interface Settings (optional)***

Im Feld **Mode** ist für AO/DI die folgende Auswahlmöglichkeit relevant:

Mögliche Werte	Bedeutung
BAP, Active Mode	Das Bandwidth Allocation Protocol (BAP) kennt drei verschiedene Möglichkeiten, eine Bandbreitenänderung zu vereinbaren. Im *Active Mode* zeigt es folgendes Verhalten: ■ Call-Request: einer der beiden Kommunikationspartner möchte einen B-Kanal zuschalten; das Zuschalten wird gegebenenfalls initiiert aber nicht akzeptiert. ■ Callback-Request: die Gegenseite wird aufgefordert, einen B-Kanal zuzuschalten; das Zuschalten wird nicht initiiert aber gegebenenfalls akzeptiert. ■ Link-Drop-Request: ein Kommunikationspartner möchte einen B-Kanal abbauen; der Abbau wird initiiert aber nicht akzeptiert.

Tabelle 7-17: **Mode** = *BAP, Active Mode*

- Wählen Sie **Mode** aus: *BAP, Active Mode*.
- Übernehmen Sie für die anderen Felder dieses Menüs die voreingestellten Werte.
- Bestätigen Sie mit **SAVE**.
- Bestätigen Sie mit **OK**.

Um die erforderliche ISDN-Rufnummer für die B-Kanal-Zuschaltung einzutragen, gehen Sie folgendermaßen vor:

- Gehen Sie zu ***WAN PARTNER*** ➧ ***ADD*** ➧ ***WAN NUMBERS*** ➧ ***ADD***.
- Geben Sie **Number** ein, z. B. ***0911123456***.
- Wählen Sie **Direction** aus: *outgoing*.
- Bestätigen Sie mit **SAVE**.

- Verlassen Sie ***WAN PARTNER*** ➧ ***ADD*** ➧ ***WAN NUMBERS*** ➧ ***ADD*** mit **Exit**.

Bei dynamischer Vergabe der IP-Adresse seitens des Service Providers, gehen Sie folgendermaßen vor:

- Gehen Sie zu ***WAN PARTNER*** ➧ ***ADD*** ➧ ***IP***.
- Wählen Sie **IP Transit Network** aus: *dynamic client*.
- Bestätigen Sie mit **SAVE**.
- Bestätigen Sie mit **SAVE**.
- Verlassen Sie ***WAN PARTNER*** mit **Exit**.
  Sie befinden sich wieder im Hauptmenü.

7.2.5 Applikationsgesteuertes Bandbreitenmanagement

Filter und Regeln

Applikationsgesteuertes Bandbreitenmanagement wird über Filter und Regeln in ähnlicher Weise konfiguriert wie Access-Listen für IP-Pakete (siehe Kapitel 9.2.8, Seite 339). Zunächst werden Filter definiert, die festlegen, welche IP-Pakete (und damit Applikationen) Einfluß auf die zur Verfügung stehende Bandbreite haben sollen. Falls mehrere Filter definiert sind, können sie mit Hilfe einer Regelkette miteinander verknüpft werden.

Gehen Sie folgendermaßen vor, um entsprechende Filter zu definieren:

- Gehen Sie zu ***IP*** ➧ ***BANDWIDTH ON DEMAND (BOD)*** ➧ ***FILTER*** ➧ ***ADD***.
- Geben Sie **Description** ein, z. B. ***mail_smtp_out***.
- Wählen Sie **Protocol** aus. z. B. ***tcp***.
- Geben Sie **Destination Address** ein, z. B. ***172.16.08.15***.
- Geben Sie **Destination Mask** ein, z. B. ***255.255.255.255***.
- Wählen Sie **Destination Port** aus: z. B. ***specify***.
- Geben Sie **Specify Port** ein, z. B. ***25*** (Port für SMTP).
- Bestätigen Sie mit **SAVE**.
  Sie sehen eine Liste aller bisher definierten Filter.

➤ Verlassen Sie ***IP*** ➧ ***BANDWIDTH ON DEMAND (BOD)*** ➧ ***FILTER*** mit **Exit**.

BOD-Regel definieren

Eine Regel für BOD wird in ähnlicher Weise festgelegt wie eine Regel für IP-Pakete (siehe Kapitel 9.2.8, Seite 339). Verschiedene Regeln bestehen normalerweise aus unterschiedlichen Filtern und können untereinander zu einer Regelkette verknüpft werden. Jede Regel zieht eine Aktion nach sich, für jede Regel kann aber auch die Richtung der Datenpakete angegeben werden, für die sie gelten soll, d. h. für gesendete oder für empfangene Datenpakete.

Gehen Sie folgendermaßen vor, um eine Regel für BOD zu definieren:

➤ Gehen Sie zu ***IP*** ➧ ***BANDWIDTH ON DEMAND (BOD)*** ➧ ***RULES FOR BOD*** ➧ ***ADD***.

Neben den bereits bekannten Feldern zur Definition von herkömmlichen Regeln (siehe Kapitel 9.2.8, Seite 339) enthält das Menü folgende Felder:

Feld	Bedeutung
Direction	Richtung der Datenpakete, auf welche die Regel angewandt werden soll. Mögliche Werte: ■ *incoming*: eingehende Datenpakete ■ *outgoing*: ausgehende Datenpakete ■ *both*: eingehende und ausgehende Datenpakete
Number of Channels	Zahl der B-Kanäle, die zugeschaltet werden sollen.

Tabelle 7-18: ***IP*** ➧ ***BANDWIDTH ON DEMAND (BOD)*** ➧ ***RULES FOR BOD*** ➧ ***ADD***

Das Feld **Action**, das angibt, wie mit einem ausgefilterten Datenpaket verfahren werden soll, enthält folgende Auswahlmöglichkeiten:

Mögliche Werte	Bedeutung
invoke M	B-Kanäle werden zugeschaltet, wenn die Regel paßt.
invoke !M	B-Kanäle werden zugeschaltet, wenn die Regel nicht paßt.

Mögliche Werte	Bedeutung
deny M	B-Kanäle werden nicht zugeschaltet, wenn die Regel paßt.
deny !M	B-Kanäle werden nicht zugeschaltet, wenn die Regel nicht paßt.
ignore	Die Regel wird ignoriert bzw. in einer Regelkette wird die Regel übersprungen.

Tabelle 7-19: **Action**

- Wählen Sie **Action** aus, z. B. ***invoke M***.
- Wählen Sie **Direction** aus, z. B. ***outgoing***.
- Wählen Sie **Number of Channels** aus, z. B. ***1***.
- Wählen Sie **Filter** aus, z. B. ***mail_smtp_out***.
- Bestätigen Sie mit **SAVE**.
- Verlassen Sie ***IP*** ➧ ***BANDWIDTH ON DEMAND (BOD)*** ➧ ***RULES FOR BOD*** mit **Exit**.
- Verlassen Sie ***IP*** ➧ ***BANDWIDTH ON DEMAND (BOD)*** mit **Exit**.

  Sie befinden sich wieder im Hauptmenü.

Um eine Regel auf ein Interface anzuwenden, gehen Sie folgendermaßen vor:

- Gehen Sie zu ***IP*** ➧ ***BANDWIDTH ON DEMAND (BOD)*** ➧ ***CONFIGURE INTERFACES FOR BOD***.
- Wählen Sie das Interface aus, auf das Sie eine Regel anwenden möchten, z. B. ***aodiclient***, und bestätigen Sie mit der **Eingabetaste**.
- Wählen Sie die Regel aus, die Sie auf dieses Interface anwenden möchten, z. B. ***mail_smtp_out***.
- Bestätigen Sie mit **SAVE**.
- Verlassen Sie ***IP*** ➧ ***BANDWIDTH ON DEMAND (BOD)*** ➧ ***CONFIGURE INTERFACES FOR BOD*** ➧ ***EDIT*** mit **Exit**.
- Verlassen Sie ***IP*** ➧ ***BANDWIDTH ON DEMAND (BOD)*** ➧ ***CONFIGURE INTERFACES FOR BOD*** mit **Exit**.

➤ Verlassen Sie ***IP*** ➧ ***BANDWIDTH ON DEMAND (BOD)*** mit **Exit**.

➤ Verlassen Sie das Menü ***IP*** mit **Exit**.

Sie befinden sich wieder im Hauptmenü.

Konfigurationsbeispiele für applikationsgesteuertes BOD (Bandwidth on Demand)

Zwei Konfigurationsbeispiele werden im folgenden dargestellt:

- Zusätzliche Bandbreite bei HTTP-Verbindungen
- Mail-Empfang auf D-Kanal beschränken

Zusätzliche Bandbreite bei HTTP-Verbindungen

Das folgende Beispiel zeigt Ihnen eine spezielle Konfiguration von **X4100/200/300** beim Verbindungsaufbau des Rechners mit der IP-Adresse 172.16.77.11 (TCP Port 80) zum Internet. Es soll immer dann in den B-Kanal-Modus mit einem B-Kanal gewechselt werden, wenn eine HTTP-Verbindung zum Internet aufgebaut wird.

Um das entsprechende Filter für BOD festzulegen, gehen Sie folgendermaßen vor:

➤ Gehen Sie zu ***IP*** ➧ ***BANDWIDTH ON DEMAND (BOD)*** ➧ ***FILTER*** ➧ ***ADD***.

➤ Geben Sie **Description** ein: *hostxy_http_out*.

➤ Wählen Sie **Protocol** aus: *tcp*.

➤ Geben Sie **Source Address** ein: *172.16.77.11*.

➤ Geben Sie **Source Mask** ein: *255.255.255.255*.

➤ Wählen Sie **Destination Port** aus: *specify*.

➤ Geben Sie **Specify Port** ein: *80*.

➤ Bestätigen Sie mit **SAVE**.

Sie sehen eine Liste aller bisher definierten Filter.

➤ Verlassen Sie ***IP*** ➧ ***BANDWIDTH ON DEMAND (BOD)*** ➧ ***FILTER*** mit **Exit**.

Um eine Regel für BOD festzulegen, gehen Sie folgendermaßen vor:

➤ Gehen Sie zu ***IP*** ➧ ***BANDWIDTH ON DEMAND (BOD)*** ➧ ***RULES FOR BOD*** ➧ ***ADD***.

- Wählen Sie **Action** aus: *invoke M*.
- Wählen Sie **Direction** aus: *outgoing*.
- Wählen Sie **Number of Channels** aus: *1*.
- Wählen Sie **Filter** aus: *hostxy_http_out (1)*.
- Bestätigen Sie mit **SAVE**.
- Verlassen Sie ***IP*** ➧ ***BANDWIDTH ON DEMAND (BOD)*** ➧ ***RULES FOR BOD*** mit **Exit**.

Interfaces festlegen

- Gehen Sie zu ***IP*** ➧ ***BOD*** ➧ ***INTERFACES***.
- Wählen Sie *AODI-partner* aus.
- Verlassen Sie ***IP*** ➧ ***BOD*** ➧ ***INTERFACES*** mit **Exit**.

  Das Filter ist festgelegt.

Mail-Empfang auf D-Kanal beschränken

Im folgenden Konfigurationsbeispiel wird der Mail-Empfang auf den D-Kanal beschränkt, es erfolgt kein Wechsel in den B-Kanal-Modus. Auch bei der Abfrage, ob neue Mails angekommen sind, wird nicht in den B-Kanal-Modus gewechselt.

Um das entsprechende Filter für BOD festzulegen, gehen Sie folgendermaßen vor:

- Gehen Sie zu ***IP*** ➧ ***BANDWIDTH ON DEMAND (BOD)*** ➧ ***FILTER*** ➧ ***ADD***.
- Geben Sie **Description** ein: *mail_pop3_in*.
- Wählen Sie **Protocol** aus: *tcp*.
- Geben Sie **Destination Address** ein: *172.16.08.15*.
- Geben Sie **Destination Mask** ein: *255.255.255.255*.
- Wählen Sie **Destination Port** aus: *specify*.
- Geben Sie **Specify Port** ein: *110*.
- Bestätigen Sie mit **SAVE**.

  Sie sehen eine Liste aller bisher definierten Filter.
- Verlassen Sie ***IP*** ➧ ***BANDWIDTH ON DEMAND (BOD)*** ➧ ***FILTER*** mit **Exit**.

Um eine Regel für BOD festzulegen, gehen Sie folgendermaßen vor:

- Gehen Sie zu ***IP*** ➧ ***BANDWIDTH ON DEMAND (BOD)*** ➧ ***RULES FOR BOD*** ➧ ***ADD***.
- Wählen Sie **Action** aus: *deny M*.
- Wählen Sie **Direction** aus: *incoming*.
- Wählen Sie **Number of Channels** aus: *1*.
- Wählen Sie **Filter** aus: *mail_pop3_in (2)*.
- Bestätigen Sie mit **SAVE**.
- Verlassen Sie ***IP*** ➧ ***BANDWIDTH ON DEMAND (BOD)*** ➧ ***RULES FOR BOD*** mit **Exit**.

Interfaces festlegen

- Gehen Sie zu ***IP*** ➧ ***BOD*** ➧ ***INTERFACES***.
- Wählen Sie *AODI-partner* aus.
- Verlassen Sie ***IP*** ➧ ***BOD*** ➧ ***INTERFACES*** mit **Exit**.

  Das Filter ist festgelegt.

7.2.6 Layer 1 Protocol (ISDN-B-Kanal)

ISDN-B-Kanal

Sie können das Layer 1 Protocol des ISDN-➧➧ **B-Kanals**, das **X4100/200/300** für Verbindungen zum WAN-Partner nutzen soll, definieren. Voreingestellt ist das Protokoll für ISDN-Datenverbindungen mit 64 kBit/s, dem Standardwert des B-Kanals. Ändern Sie die Einstellung nur, wenn dies ausdrücklich erforderlich ist.

Die Konfiguration erfolgt in ***WAN PARTNER*** ➧ ***EDIT*** ➧ ***ADVANCED SETTINGS***:

Feld	Bedeutung
Layer 1 Protocol	Legt fest, welches Layer 1 Protocol **X4100/200/300** 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 7-20: ***WAN PARTNER*** ➧ ***EDIT*** ➧ ***ADVANCED SETTINGS***

Für eingehende Rufe, die nicht anhand der Calling Party's Number identifiziert werden können, verwendet **X4100/200/300** als Layer 1 Protocol die Einstellungen unter **Item** in ***CM-1BRI, ISDN S0*** ➧ ***INCOMING CALL ANSWERING*** (siehe "Incoming Call Answering", Seite 125).

Layer 1 Protocol enthält folgende Auswahlmöglichkeiten:

Mögliche Werte	Bedeutung
ISDN 64 kbps	Für ISDN-Datenverbindungen mit 64 kBit/s. Dies ist der Standardwert.
ISDN 56 kbps	Für ISDN-Datenverbindungen mit 56 kBit/s.
Modem	(nur nutzbar bei eingebauter Erweiterungskarte mit Ressourcenkarte mit Digitalmodems) Weist eingehende analoge Rufe dem Dienst PPP-Routing zu. Das digitale Modem auf der Ressourcenkarte, das diesen Ruf entgegennimmt, verwendet die Einstellungen für Modemprofil 1, die im Menü ***MODEM*** ➧ ***PROFILE CONFIGURATION*** ➧ ***PROFILE 1*** getroffen wurden.
DOVB	Data transmission Over Voice Bearer – nützlich z. B. in den USA, wo Sprachverbindungen manchmal billiger sind als Datenverbindungen.

Mögliche Werte	Bedeutung
V.110 (1200 ... 38400)	Für GSM-Verbindungen mit V.110 und mit Bit-Raten von 1200 Bit/s, 2400 Bit/s,..., 38400 Bit/s.
Modem Profile 1 ... 8	(nur verfügbar bei eingebauter Erweiterungskarte mit Ressourcenkarte mit Digitalmodems) Weist eingehende analoge Rufe dem Dienst PPP-Routing zu. Das digitale Modem auf der Ressourcenkarte, das diesen Ruf entgegennimmt, verwendet die Einstellungen für Modemprofile 1... 8, die im Menü ***MODEM*** ➧ ***PROFILE CONFIGURATION*** ➧ ***PROFILE 1...8*** getroffen wurden.
PPTP PNS	Für VPN-Schnittstelle.
PPP over Ethernet (PPPoE)	Für Verbindungen mit xDSL (siehe Kapitel 6.2.3, Seite 138).
AO/DI	Für die Nutzung von Always On/Dynamic ISDN (AO/DI, siehe Kapitel 7.2.4, Seite 198).
PPP over PPTP	Für Verbindungen mit xDSL z. B. in Österreich (siehe "Beispiel 2: Telekom Austria (High-Speed-Internet-Anschluß)", Seite 144.

Tabelle 7-21: **Layer 1 Protocol**

Die meisten Einträge von **Layer 1 Protocol** entsprechen den Einträgen von **Item** in ***CM-1BRI, ISDN S0*** ➧ ***INCOMING CALL ANSWERING*** (siehe "Incoming Call Answering", Seite 125).

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**.

Das von Ihnen gewählte Protokoll ist konfiguriert.

7.2.7 IP Transit Network

Wenn Sie einen WAN-Partner auf **X4100/200/300** eintragen, gibt es verschiedene Möglichkeiten, die IP-Adresse des Partnernetzes anzugeben:

- Sie geben ➤➤ **IP-Adresse** und ➤➤ **Netzmaske** des Partners bzw. Partnernetzes an. Dazu müssen Sie diese natürlich kennen.
- Sie verwenden sowohl für **X4100/200/300** als auch für den WAN-Partner jeweils eine zusätzliche ISDN-IP-Adresse. Damit bauen Sie während der Verbindung ein virtuelles IP-Netzwerk auf, ein sogenanntes Transitnetzwerk. Diese Einstellung benötigen Sie normalerweise nicht, nur bei manchen Spezialkonfigurationen ist sie notwendig.
- Sie weisen dem WAN-Partner dynamisch für die Dauer der Verbindung eine IP-Adresse aus einem festgelegten IP-Address-Pool zu.
- Sie lassen sich vom WAN-Partner dynamisch für die Dauer der Verbindung eine IP-Adresse zuweisen.

Grafische Darstellung mit Beispielwerten:

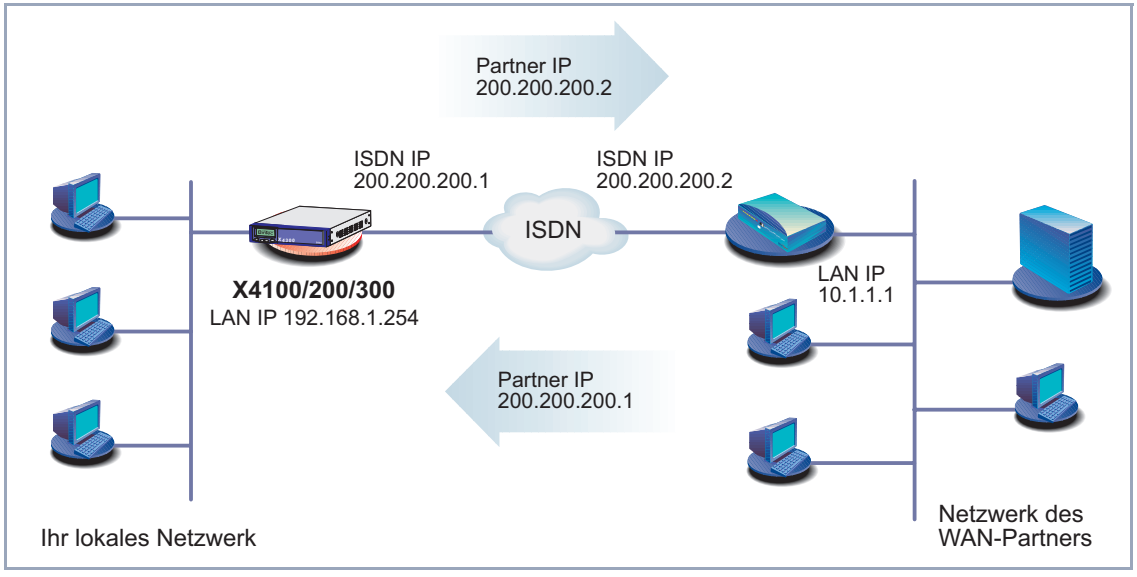


Bild 7-1: LAN-LAN-Kopplung mit Transitnetzwerk

Die Konfiguration erfolgt in ***WAN PARTNER*** ➧ ***EDIT*** ➧ ***IP***:

Feld	Bedeutung
IP Transit Network	Legt fest, ob **X4100/200/300** ein Transitnetzwerk zum WAN-Partner aufbaut. Mögliche Werte: siehe Tabelle 7-23, Seite 216.
local IP Address	LAN-IP-Adresse von **X4100/200/300**. Erscheint nur bei folgendem Wert für **IP Transit Network**: *no*. Im Normalfall müssen Sie hier keinen Eintrag machen. Ausnahme: Sie richten mehrere WAN-Partner ein und verwenden für einen oder mehrere WAN-Partner ein Transitnetzwerk, für die anderen WAN-Partner kein Transitnetzwerk. Dann geben Sie bei allen WAN-Partnern ohne Transitnetzwerk die **local IP Address** (LAN-IP-Adresse) an.

Feld	Bedeutung
local ISDN IP Address	ISDN-IP-Adresse von **X4100/200/300** 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 bzw. LAN-IP-Adresse (Host).
Partner's LAN Netmask	Netzmaske des LANs bzw. Netzmaske des Hosts des WAN-Partners. Wenn Sie keinen Eintrag machen, trägt **X4100/200/300** eine Standardnetzmaske für die unter **Partner's LAN IP Address** verwendete Netzklasse ein.

Tabelle 7-22: ***WAN Partner*** ➧ ***Edit*** ➧ ***IP***

IP Transit Network enthält folgende Auswahlmöglichkeiten:

Mögliche Werte	Bedeutung
yes	Verwendung eines Transitnetzwerkes.
dynamic client	**X4100/200/300** erhält seine IP-Adresse für die Dauer der Verbindung vom WAN-Partner.
dynamic server	**X4100/200/300** weist dem ➤➤ **Remote**-WAN-Partner für die Dauer der Verbindung eine IP-Adresse zu. Dazu muß **X4100/200/300** als dynamischer IP-Address-Server konfiguriert sein, d. h. über einen IP-Address-Pool verfügen (siehe Kapitel 7.1.1, Seite 180).
no	Kein Transitnetzwerk. Für die meisten WAN-Partner ist diese Einstellung ausreichend.

Tabelle 7-23: **IP Transit Network**

ToDo Gehen Sie folgendermaßen vor:

➤ Gehen Sie zu ***WAN Partner*** ➧ ***Edit*** ➧ ***IP***.

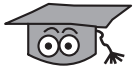
- Wählen Sie **IP Transit Network** aus.
- Geben Sie gegebenenfalls **local IP Address** ein.
- Geben Sie gegebenenfalls **local ISDN IP Address** ein.
- Geben Sie gegebenenfalls **Partner's ISDN IP Address** ein.
- Geben Sie gegebenenfalls **Partner's LAN IP Address** ein.
- Geben Sie gegebenenfalls **Partner's LAN Netmask** ein.
- Bestätigen Sie mit **SAVE**.

  Die IP-Adressen sind eingetragen.

7.2.8 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 verwendet, um Host-Namen bzw. ➤➤ **NetBIOS**-Namen in IP-Adressen zu übersetzen (Namensauflösung). Domain-Name-Server bilden eine hierarchische Baumstruktur. Sobald eine Anfrage an einen 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.



Falls Sie die Funktion DNS-Proxy nutzen, kann **X4100/200/300** u. a. einmal aufgelöste Namen und IP-Adressen im Cache speichern und überprüft bei einer Anfrage zunächst, ob die gesuchte Adresse aus dem Cache beantwortet werden kann. Damit werden die Kosten, die durch Aufbau von WAN-Verbindungen zu Name-Servern außerhalb des LANs entstehen, niedrig gehalten und die Performanz im LAN optimiert, da Anfragen an häufig genutzte oder schon einmal aufgelöste Adressen von **X4100/200/300** selbst beantwortet werden. Die Konfiguration des DNS-Proxy finden Sie in Kapitel 7.3.2, Seite 238.

Bei Eintragen eines WAN-Partners auf **X4100/200/300** können Sie festlegen, ob **X4100/200/300** Anfragen nach WINS- bzw. DNS-IP-Adressen sendet oder beantwortet.

Die Konfiguration erfolgt in den Menüs ***IP*** ➧ ***STATIC SETTINGS*** und ***WAN PARTNER*** ➧ ***EDIT*** ➧ ***IP*** ➧ ***ADVANCED SETTINGS***.

Menü ***IP*** ➧ ***STATIC SETTINGS***:

Feld	Bedeutung
Primary Domain Name Server	IP-Adresse von **X4100/200/300**s erstem globalen Domain-Name-Server (DNS).
Secondary Domain Name Server	IP-Adresse eines weiteren globalen Domain-Name-Servers.
Primary WINS	IP-Adresse von **X4100/200/300**s erstem globalen WINS (Windows Internet Name Server) bzw. NBNS (NetBIOS Name Server).
Secondary WINS	IP-Adresse eines weiteren globalen WINS bzw. NBNS.

Tabelle 7-24: ***IP*** ➧ ***STATIC SETTINGS***

Menü ***WAN PARTNER*** ➧ ***EDIT*** ➧ ***IP*** ➧ ***ADVANCED SETTINGS***:

Feld	Bedeutung
Dynamic Name Server Negotiation	Legt fest, ob **X4100/200/300** IP-Adressen für **Primary Domain Name Server**, **Secondary Domain Name Server**, **Primary WINS** und **Secondary WINS** im Falle einer dynamischen Name-Server-Aushandlung vom WAN-Partner erhält oder an den WAN-Partner sendet.

Tabelle 7-25: ***WAN PARTNER*** ➧ ***EDIT*** ➧ ***IP*** ➧ ***ADVANCED SETTINGS***

Das Feld **Dynamic Name Server Negotiation** enthält folgende Auswahlmöglichkeiten:

Mögliche Werte	Bedeutung
off	**X4100/200/300** sendet und beantwortet keine Anfragen nach WINS- bzw. DNS-IP-Adressen.

Mögliche Werte	Bedeutung
yes	Das Verhalten ist an den Modus für Vergabe/ Empfang einer IP-Adresse gekoppelt. Einstellung in ***WAN PARTNER*** ➧ ***EDIT*** ➧ ***IP*** unter **IP Transit Network**: ■ **X4100/200/300** sendet Anfragen nach Name-Server-Adressen an den WAN-Partner, falls *dynamic client* ausgewählt ist. ■ **X4100/200/300** beantwortet Anfragen des WAN-Partners nach Name-Server-Adressen, falls *dynamic server* ausgewählt ist. ■ **X4100/200/300** beantwortet, aber sendet keine Anfragen nach Name-Server-Adressen, falls *yes* oder *no* ausgewählt ist.
client (receive)	**X4100/200/300** sendet Anfragen nach Name-Server-Adressen an den WAN-Partner.
server (send)	**X4100/200/300** beantwortet Anfragen des WAN-Partners nach Name-Server-Adressen.

Tabelle 7-26: **Dynamic Name Server Negotiation**

WINS, DNS im LAN

Falls Sie einen Domain-Name-Server bzw. Windows Internet 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 vorgenommen haben (siehe Kapitel 7.3.2, Seite 238):

- 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 **X4100/200/300** die eingetragenen Name-Server-Adressen dem WAN-Partner mitteilen soll (Servermodus) bzw.

wenn bei Verbindungen zum WAN-Partner andere Name-Server-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 die gewünschte Funktion für **Dynamic Name Server Negotiation** aus.
- Bestätigen Sie mit **OK**.
- Bestätigen Sie mit **SAVE**.

Wenn Sie keinen Secondary DNS bzw. WINS Server haben, können Sie ein zweites Mal die IP-Adresse des Primary DNS bzw. WINS Servers in das Feld **Secondary Domain Name Server** bzw. **Secondary WINS** eingeben.

Dies kann für die Verbindung mit manchen DFÜ-Clients notwendig sein.

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.

7.2.9 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 sogenannten Routing-Tabelle (siehe Kapitel 6.3.2, Seite 165) entscheidet der Router, auf welchem Weg (Route) er das Datenpaket weiterschickt, damit es möglichst schnell (mit möglichst wenigen Zwischenstationen) und günstig ans Ziel gelangt. Die Eintragungen der Routing-Tabelle können entweder statisch festgelegt werden, oder es erfolgt eine laufende Aktualisierung der Routing-Tabelle durch dynamischen Austausch der Routing-In-

formationen zwischen mehreren Routern. Diesen Austausch regelt ein sogenanntes 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. **X4100/200/300** unterstützt sowohl Version 1 als auch Version 2 von RIP, wahlweise einzeln oder gemeinsam.

RIP wird für LAN und WAN separat konfiguriert.

Aktiv und Passiv

Man kann dabei aktive und passive 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. **X4100/200/300** kann beides.

WAN-Partner

Wenn Sie mit einem WAN-Partner Empfangen und/oder Senden von RIP-Paketen vereinbaren, kann **X4100/200/300** mit den Routern im LAN des WAN-Partners dynamisch Routing-Informationen austauschen.

Der Empfang von Routing-Tabellen über RIP ist eventuell eine Sicherheitslücke, da fremde Rechner bzw. Router die Routing-Funktionalität von **X4100/200/300** verändern können.

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

Die Konfiguration erfolgt in den Menüs ***WAN PARTNER*** ➧ ***EDIT*** ➧ ***IP*** ➧ ***ADVANCED SETTINGS*** bzw. ***CM-100BT, FAST ETHERNET*** ➧ ***ADVANCED SETTINGS***:

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 7-27: ***WAN PARTNER*** ➧ ***EDIT*** ➧ ***IP*** ➧ ***ADVANCED SETTINGS*** bzw. ***CM-100BT, FAST ETHERNET*** ➧ ***ADVANCED SETTINGS***

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 7-28: **RIP Send** bzw. **RIP Receive**

ToDo Gehen Sie folgendermaßen vor:

- Gehen Sie zu ***WAN Partner*** ➧ ***Edit*** ➧ ***IP*** ➧ ***Advanced Settings***.
- Wählen Sie die gewünschte Funktion von **RIP Send** aus.
- Wählen Sie die gewünschte Funktion von **RIP Receive** aus.
- Bestätigen Sie mit **OK**.
- Bestätigen Sie mit **SAVE**, bis Sie sich im Hauptmenü befinden.
- Gehen Sie zu ***CM-100BT, Fast Ethernet*** ➧ ***Advanced Settings***.
- Wählen Sie **RIP Send** aus.
- Wählen Sie **RIP Receive** aus.
- Bestätigen Sie mit **SAVE**.

7.2.10 Komprimierung

Datenkomprimierung Mit Hilfe von ➤➤ **Datenkomprimierung** können Sie den Datendurchsatz erhöhen und damit die Verbindungskosten senken. **X4100/200/300** unterstützt

mehrere Möglichkeiten, abhängig von der gewählten ➤➤ **Enkapsulierung**, z. B. PPP (siehe Kapitel 6.3, Seite 147):

- ➤➤ **STAC**:
  Durch den in **X4100/200/300** 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). Nützlich zu Einwahl bei einem Windows-Remote-Access-Server.
- Van-Jacobson-Header-Komprimierung (➤➤ **VJHC**):
  Reduziert die Größe von ➤➤ **TCP/IP**-Paketen. Van-Jacobson-Header-Komprimierung kann zusätzlich zu den obengenannten Kompressionsalgorithmen eingesetzt werden.

Sollte eine Gegenstelle keine Datenkomprimierung unterstützen bzw. die Unterstützung nicht aktiviert haben, so erkennt **X4100/200/300** dies innerhalb der ➤➤ **PPP**-Verhandlungsphase und deaktiviert die Datenkomprimierung für diese Verbindung.

Die Konfiguration erfolgt in den Menüs ***WAN PARTNER*** ➧ ***EDIT*** und ***WAN PARTNER*** ➧ ***EDIT*** ➧ ***IP*** ➧ ***ADVANCED SETTINGS***.

Menü ***WAN PARTNER*** ➧ ***EDIT***:

Feld	Bedeutung
Compression	Legt die Art der Komprimierung für Verbindungen mit dem WAN-Partner fest.

Tabelle 7-29: ***WAN PARTNER*** ➧ ***EDIT***

Das Feld **Compression** enthält folgende Auswahlmöglichkeiten:

Mögliche Werte	Bedeutung
none	Keine Komprimierung.

Mögliche Werte	Bedeutung
STAC	Ermöglicht STAC-Datenkomprimierung (wenn **Encapsulation** = *PPP*).
MS-STAC	Nützlich für STAC-Datenkomprimierung bei Einwahl auf einen Windows-Remote-Access-Server (wenn **Encapsulation** = *PPP*).

Tabelle 7-30: Compression

Menü ***WAN Partner*** ➧ ***Edit*** ➧ ***IP*** ➧ ***Advanced Settings***:

Feld	Bedeutung
Van Jacobson Header Compression	Ermöglicht VJHC.

Tabelle 7-31: ***WAN Partner*** ➧ ***Edit*** ➧ ***IP*** ➧ ***Advanced Settings***

STAC, MS-STAC

Gehen Sie folgendermaßen vor, um STAC oder MS-STAC einzustellen:

- Gehen Sie zu ***WAN Partner*** ➧ ***Edit***.
- Wählen Sie die gewünschte **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**, bis Sie sich im Hauptmenü befinden. Die Einstellungen sind temporär gespeichert und aktiviert.

7.2.11 Proxy ARP (Address Resolution Protocol)

ARP-Requests

Mit Hilfe von ➤➤ **Proxy ARP** kann **X4100/200/300** ➤➤ **ARP**-Requests aus dem eigenen LAN und aus dem LAN definierter WAN-Partnern beantworten.

Wenn ein Host im LAN zu einem anderen Host im LAN oder zu einem WAN-Partner eine Verbindung aufbauen will, aber dessen Hardware-Adresse nicht kennt, sendet er einen sogenannten ARP-Request als ➤➤ **Broadcast** ins Netz. Wenn auf **X4100/200/300** Proxy ARP aktiviert ist und der gewünschte Host über eine als Host-Route definierte WAN-Verbindung erreichbar ist, beantwortet **X4100/200/300** den ARP-Request mit seiner eigenen Hardware-Adresse. Dies ist für den Verbindungsaufbau ausreichend: Die ➤➤ **Datenpakete** werden an **X4100/200/300** geschickt, der sie dann an den gewünschten Host weiterleitet.

Grafische Darstellung:

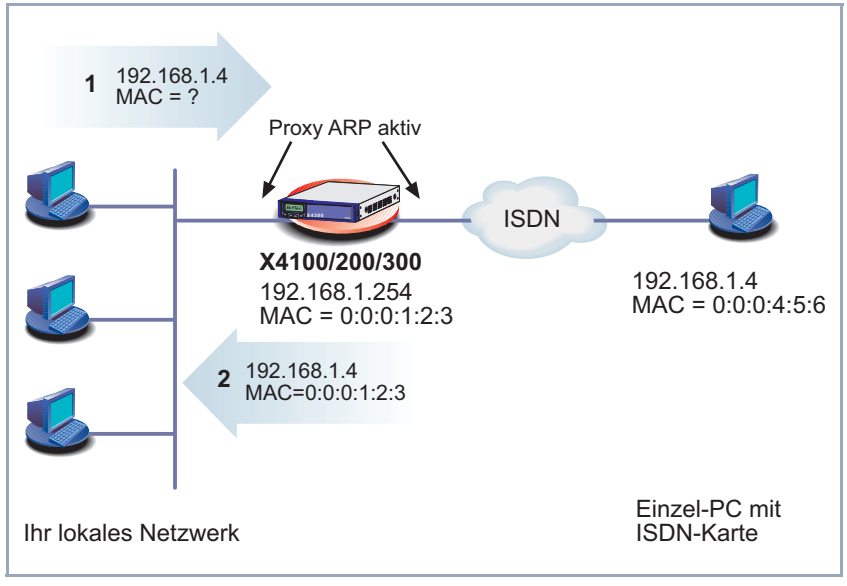


Bild 7-2: Proxy ARP

Die Konfiguration erfolgt in:

- ***WAN Partner*** ➧ ***Edit*** ➧ ***IP*** ➧ ***Advanced Settings***
- ***CM-100BT, Fast Ethernet*** ➧ ***Advanced Settings***

Folgendes Feld finden Sie in beiden Menüs:

Feld	Bedeutung
Proxy Arp	Ermöglicht **X4100/200/300**, ARP-Requests aus dem eigenen LAN und von Hosts definierter WAN-Partner zu beantworten.

Tabelle 7-32: ***WAN Partner*** ➧ ***Edit*** ➧ ***IP*** ➧ ***Advanced Settings*** bzw. ***CM-100BT, Fast Ethernet*** ➧ ***Advanced Settings***

Proxy Arp in ***WAN Partner*** ➧ ***Edit*** ➧ ***IP*** ➧ ***Advanced Settings*** enthält folgende Auswahlmöglichkeiten:

Mögliche Werte	Bedeutung
off	Deaktiviert Proxy ARP für diesen WAN-Partner.
on (up or dormant)	**X4100/200/300** beantwortet einen ARP-Request nur, wenn der Status der Verbindung zum WAN-Partner *up* (aktiv) oder *dormant* (ruhend) ist. Bei *dormant* beantwortet **X4100/200/300** lediglich den ARP-Request, der Verbindungsaufbau erfolgt erst, wenn jemand tatsächlich die Route nutzen will.
on (up only)	**X4100/200/300** beantwortet einen ARP-Request nur, wenn der Status der Verbindung zum WAN-Partner *up* (aktiv) ist, wenn also bereits eine Verbindung zum WAN-Partner besteht.

Tabelle 7-33: **Proxy Arp**

Proxy Arp in ***CM-100BT, Fast Ethernet*** ➧ ***Advanced Settings*** enthält folgende Auswahlmöglichkeiten:

Mögliche Werte	Bedeutung
off	Deaktiviert Proxy ARP über die LAN-Schnittstelle.

Mögliche Werte	Bedeutung
on	Ermöglicht Proxy ARP über die LAN-Schnittstelle.

Tabelle 7-34: **Proxy Arp**

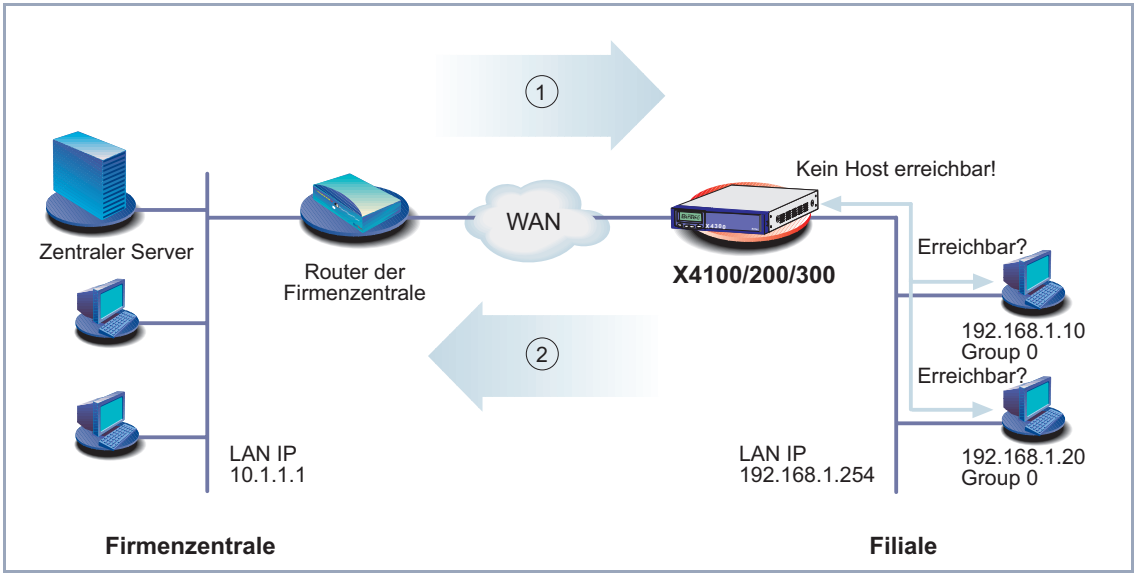
ToDo Gehen Sie folgendermaßen vor:

- Gehen Sie zu ***WAN Partner*** ➧ ***Edit*** ➧ ***IP*** ➧ ***Advanced Settings***.
- Wählen Sie die gewünschte Funktion für **Proxy Arp** aus.
- Bestätigen Sie mit **SAVE**, bis Sie sich im Hauptmenü befinden.
- Gehen Sie zu ***CM-100BT, Fast Ethernet*** ➧ ***Advanced Settings***.
- Wählen Sie die gewünschte Funktion für **Proxy Arp** aus.
- Bestätigen Sie mit **SAVE**, bis Sie sich im Hauptmenü befinden.

7.2.12 Keepalive Monitoring

LAN-LAN-Kopplung Wenn Sie zwei (oder mehrere) LANs über eine Wählverbindung gekoppelt haben – z. B. das LAN der Firmenzentrale mit dem LAN einer Filiale (Bild 7-3, Seite 228) – befindet sich häufig ein zentraler Server im LAN der Firmenzentrale. Wenn dieser zentrale Server so konfiguriert ist, daß er regelmäßig WAN-Verbindungen zu **X4100/200/300** im LAN der Filiale aufbaut, z. B. um Daten zu aktualisieren, dann sind diese Verbindungen überflüssig (aber leider nicht kostenlos), wenn keiner der Hosts in der Filiale erreichbar ist, z. B. weil alle Rechner ausgeschaltet sind. Da erst nach dem Aufbau der Verbindung festgestellt werden kann, daß die Hosts nicht erreichbar sind, entstehen Kosten für den Rufenden, also für die Firmenzentrale.

Grafische Darstellung des Keepalive Monitoring:



1	Versuch eines Verbindungs-aufbaus	2	**X4100/200/300** ist "besetzt", keine Verbindung möglich

Bild 7-3: Keepalive Monitoring

Kosten senken

Mit der Funktion "Keepalive Monitoring" können Sie **X4100/200/300** in der Filiale so konfigurieren, daß unnötige WAN-Verbindungen von der Firmenzentrale zur Filiale vermieden werden. In regelmäßigen, einstellbaren Abständen überprüft **X4100/200/300**, ob die zu überwachenden Hosts im LAN der Filiale erreichbar sind. Wenn nach drei aufeinanderfolgenden Versuchen keiner der zu überprüfenden Hosts auf eine entsprechende Anfrage antwortet, wird der Ruf von "Zentraler Server" von **X4100/200/300** nicht angenommen, indem **X4100/200/300** die Schnittstelle zum WAN-Partner "Firmenzentrale" deaktiviert. Es entstehen also keine Kosten für eine Verbindung, die ohnehin überflüssig gewesen wäre.

In manchen Ländern (z. B. Schweiz) können trotz Nutzung von Keepalive Monitoring Kosten für diese vergeblichen Einwahlversuche anfallen.

Wenn alle Rechner im LAN der Filiale inaktiv waren, wird beim Einschalten eines zu überwachenden Rechners nicht automatisch sofort eine Verbindung zur Firmenzentrale aufgebaut. Erst wenn **X4100/200/300** die Erreichbarkeit eines Rechners registriert hat, wird die Schnittstelle zum WAN-Partner "Firmenzentrale" aktiviert, ein Verbindungsaufbau durch die Firmenzentrale ist möglich. Wieviel Zeit vergeht, bis **X4100/200/300** die erneute Erreichbarkeit signalisiert, ist abhängig vom eingestellten Überwachungsintervall (**Interval**).

Der entsprechende WAN-Partner, also z. B. die Firmenzentrale (Bild 7-3, Seite 228), muß auf **X4100/200/300** per CLID (Calling Line Identification) identifiziert werden können. Wenn dies nicht der Fall ist, ist der beschriebene Nutzeffekt von "Keepalive Monitoring" nicht gegeben.

Keepalive Monitoring kann auf **X4100/200/300** nicht für WAN-Partner eingerichtet werden, die über einen RADIUS-Server authentisiert werden!

Die Konfiguration erfolgt in ***SYSTEM*** ➧ ***KEEPALIVE MONITORING*** ➧ **ADD**:

Feld	Bedeutung
Group	Definiert eine Gruppe von Hosts, deren Erreichbarkeit von **X4100/200/300** überwacht werden soll. Jeder zu überwachende Host wird einer Gruppe zugeordnet. Insgesamt können zehn Gruppen mit jeweils bis zu zehn Hosts angelegt werden. Mögliche Werte: *0* ... *9*
IPAddress	Definiert einen Host, der von **X4100/200/300** überwacht werden soll.

Feld	Bedeutung
Interval	Definiert ein Zeitintervall in Sekunden, welches zur Überprüfung der Erreichbarkeit von Hosts verwendet werden soll (Standardwert: *300 s*). Innerhalb einer Gruppe wird das kleinste **Interval** verwendet.
DownAction	Definiert, wie der Status der unter **FirstIfIndex** und **Range** festgelegten **X4100/200/300**-Schnittstellen gesetzt wird, wenn alle Hosts einer Gruppe nicht erreichbar sind. Mögliche Werte: ■ *down* (Standardwert): Schnittstellen werden deaktiviert. ■ *up*: Schnittstellen werden aktiviert. Wenn mindestens ein Host einer Gruppe wieder erreichbar ist, wird der Status der Schnittstellen wieder auf den ursprünglichen Wert gesetzt.
FirstIfIndex	Definiert die erste Schnittstelle eines Schnittstellen-Bereiches auf **X4100/200/300**, für welche die unter **DownAction** festgelegte Aktion ausgeführt werden soll. Mögliche Werte: *10001* ... *15000* (Standardwert: *10001*). Für Wählverbindungen zu WAN-Partnern sind Schnittstellen mit Indizes von 10001 bis 15000 vorgesehen. Der Standardwert *10001* bezeichnet die Schnittstelle zum ersten auf **X4100/200/300** konfigurierten WAN-Partner (Wählverbindung). Die Indizes anderer Schnittstellen finden Sie in der **Software Reference**.

Feld	Bedeutung
Range	Definiert den Bereich von Schnittstellen auf **X4100/200/300**, für welche die unter **DownAction** festgelegte Aktion ausgeführt werden soll. Wenn Sie **FirstIfIndex** = *10001* und **Range** = *0* einstellen, ist nur die Schnittstelle mit dem Index 10001 betroffen. Wenn Sie **FirstIfIndex** = *10001* und **Range** = *4999* (Standardwert) einstellen, sind die Schnittstellen mit den Indizes 10001 bis 15000 betroffen.

Tabelle 7-35: ***SYSTEM*** ➧ ***KEEPALIVE MONITORING*** ➧ **ADD**

In ***SYSTEM*** ➧ ***KEEPALIVE MONITORING*** sind alle Hosts aufgelistet, die per Keepalive Monitoring überwacht werden. Unter **State** ist dabei die Erreichbarkeit der Hosts aufgelistet: *alive*, wenn der Host bei der letzten Überprüfung erreichbar war, *down*, wenn er nicht erreichbar war.

ToDo Gehen Sie folgendermaßen vor, um das in Bild 7-3, Seite 228 dargestellte Beispiel zu konfigurieren:

- Gehen Sie zu ***SYSTEM*** ➧ ***KEEPALIVE MONITORING*** ➧ **ADD**, um den ersten Host hinzuzufügen, der mit Keepalive Monitoring von **X4100/200/300** überwacht werden soll.
- Geben Sie **Group** ein: ***0***.
- Geben Sie **IPAddress** ein: ***192.168.1.10***.
- Geben Sie **Interval** ein, z. B. ***300***.
- Wählen Sie **DownAction** aus: ***down***.
- Geben Sie **FirstIfIndex** ein: ***10001***.
- Geben Sie **Range** ein: ***4999***.
- Bestätigen Sie mit **SAVE**.
- Fügen Sie mit **ADD** den zweiten Host hinzu.

- Geben Sie **Group** ein: ***0***.
- Geben Sie **IPAddress** ein: ***192.168.1.20***.
- Geben Sie **Interval** ein, z. B. ***300***.
- Wählen Sie **DownAction** aus: ***down***.
- Geben Sie **FirstIfIndex** ein: ***10001***.
- Geben Sie **Range** ein: ***4999***.
- Bestätigen Sie mit **SAVE**.

Mit diesen Einstellungen erreichen Sie, daß **X4100/200/300** in Abständen von 300 Sekunden die Hosts 192.168.1.10 und 192.168.1.20 auf Ihre Erreichbarkeit überprüft. Wenn nach drei aufeinanderfolgenden Versuchen keiner der beiden Hosts erreichbar ist, werden alle Schnittstellen auf **X4100/200/300** für Wählverbindungen zu WAN-Partnern deaktiviert. Die Überprüfung der Hosts durch **X4100/200/300** geht mit dem Zeitintervall 300 s weiter und sobald mindestens einer wieder erreichbar ist, aktiviert **X4100/200/300** die Schnittstellen wieder.

7.3 Grundlegende IP-Einstellungen

Hier finden Sie einige grundlegende Einstellungen, die Sie auf **X4100/200/300** festlegen können:

- Beziehen der Systemzeit (Kapitel 7.3.1, Seite 233)
- Namensauflösung (➤➤ **DNS**) auf **X4100/200/300** (Kapitel 7.3.2, Seite 238)
- ➤➤ **Port**-Nummern (Kapitel 7.3.3, Seite 256)
- ➤➤ **BOOTP** Relay Agent (Kapitel 7.3.4, Seite 258)

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.

Sie können die Systemzeit

- automatisch beziehen, z. B. über ISDN oder über einen Time-Server (siehe "Systemzeit automatisch beziehen", Seite 234).
- manuell auf **X4100/200/300** einstellen (siehe "Systemzeit manuell einstellen", Seite 237).

Systemzeit automatisch beziehen

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 **X4100/200/300** die Angabe als Anzahl von Stunden und wandelt sie nach Bestätigen mit **SAVE** automatisch in die entsprechende Anzahl von Sekunden um. Beachten Sie: Wenn Sie *ISDN* als **Time Protocol** wählen, sollten Sie den **Time Offset** auf *0* setzen. Wenn Sie **Time Offset (sec)** verändern (Zeit zurückstellen), sollte kein Datenfluß bestehen.

Feld	Bedeutung
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 **X4100/200/300** die Angabe als Anzahl von Stunden und wandelt sie nach dem Drükken von **SAVE** 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.
Time Server	IP-Adresse des Time-➤➤ **Servers**, den **X4100/200/300** nutzt. **Time Server** wird nicht benötigt, wenn Sie *ISDN* als **Time Protocol** einstellen.

Tabelle 7-36: ***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	Systemzeit per SNTP (Simple Network Time Protocol, RFC 1769) über UDP.
ISDN	Systemzeit aus ISDN-➤➤ **D-Kanal** (kostenlos).
none	Keine Systemzeit beziehen.

Tabelle 7-37: **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**.

  Mit dem Aufbau der ersten ISDN-Verbindung bezieht **X4100/200/300** 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 Host-Name für **Time Server** ein.
- Bestätigen Sie mit **SAVE**.

  X4100/200/300 bezieht somit die Systemzeit über einen Time-Server. Alle 24 Stunden gleicht **X4100/200/300** 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 **X4100/200/300** der Time-Server der **DIME Tools** auf Ihrem PC aktiv ist.

Wenn Ihr Rechner keine feste IP-Adresse hat, sondern eine wechselnde IP-Adresse via ➧➧ **DHCP** dynamisch zugewiesen bekommt, können Sie Ihren Rechner nicht als Time-Server verwenden.

Systemzeit manuell einstellen

Die Konfiguration erfolgt in ***SYSTEM*** ➧ ***TIME AND DATE***:

Feld	Bedeutung
Time is currently controlled by:	Zeigt an, welche Einstellungen für ein automatisches Beziehen der Systemzeit unter ***IP*** ➧ ***STATIC SETTINGS*** festgelegt sind.
Current Time:	Zeigt die aktuell auf **X4100/200/300** eingestellte Systemzeit an (Datum und Uhrzeit).
New Time:	Hier wird die neue Uhrzeit eingegeben, die **X4100/200/300** verwenden soll (Stunden:Minuten).
New Date:	Hier wird das neue Datum eingegeben, das **X4100/200/300** verwenden soll (Monat/Tag/Jahr).

Tabelle 7-38: ***SYSTEM*** ➧ ***TIME AND DATE***

Gehen Sie folgendermaßen vor, um die Systemzeit auf **X4100/200/300** manuell einzugeben:

Wenn auf **X4100/200/300** zusätzlich eine Methode zum automatischen Beziehen der Zeit festgelegt ist, haben die auf diese Weise erhaltenen Werte höhere Priorität. D. h. falls **X4100/200/300** ein entsprechendes Zeitsignal erhält (z. B. von einem Time-Server), wird eine evtl. manuell eingegebene Systemzeit überschrieben.

- Gehen Sie zu ***SYSTEM*** ➧ ***TIME AND DATE***.
- Geben Sie **New Time** ein.
- Geben Sie **New Date** ein.
- Bestätigen Sie die neue Systemzeit mit **SET**.

  Unter **Current Time:** wird die auf **X4100/200/300** neu eingestellte Systemzeit angezeigt.

7.3.2 Namensauflösung – X4100/200/300 mit DNS-Proxy

Wozu Namensauflösung?

IP-Adresse = ?

Namensauflösung ist erforderlich, um Host-Namen in einem LAN oder im Internet in IP-Adressen zu übersetzen. Wenn Sie also z. B. den Host "Goofy" in Ihrem LAN ansprechen möchten (z. B. mit `telnet` und `ping`) oder die ➤➤ **URL** "http://www.bintec.de" in Ihren Internet-Browser eingeben, benötigen Sie jeweils die dazugehörige IP-Adresse, um die geforderte Verbindung aufbauen zu können. Dazu gibt es im allgemeinen verschiedene Möglichkeiten, z. B.:

- DNS (Domain Name Service):
  Auf einem DNS-Server werden zu Host-Namen die entsprechenden IP-Adressen in Form von DNS-Records hinterlegt und bei einer entsprechenden Anfrage aufgelöst, d. h. ein DNS-Record mit der zum Namen gehörigen IP-Adresse wird vom Name-Server an die Quelle der Anfrage geschickt. Name-Server bilden eine hierarchische Baumstruktur. Wenn also ein Name-Server einen Namen nicht auflösen kann, fragt er bei einem übergeordneten Name-Server nach usw..

- HOSTS-Dateien:
  Auf HOSTS-Dateien, die sich auf den PCs im LAN befinden, legen Sie eine Tabelle von Host-Namen mit den dazugehörigen IP-Adressen an. Damit sind zur Auflösung dieser Namen Verbindungen zu DNS-Servern überflüssig. Da man die Aktualisierung der HOSTS-Dateien auf jedem PC durchführen muß, ist diese Methode zur Namensauflösung nicht sehr praktikabel.

In der Praxis wird zur Namensauflösung häufig der DNS-Server des Internet Service Providers genutzt.

Vorteile der Namensauflösung mit X4100/200/300

X4100/200/300 verfügt zur Namensauflösung (Port 53) über folgende Funktionen und Möglichkeiten:

- DNS-Proxy, um DNS-Anfragen an den geeigneten DNS-Server weiterzuleiten.
- DNS-Cache, um die Ergebnisse von DNS-Anfragen zu speichern.
- Statische Namenseinträge, um Zuordnungen von Namen zu IP-Adressen festzulegen.
- Filterfunktion, um eine Auflösung von bestimmten Namen zu verhindern.
- Monitoring mit dem Setup Tool, um einen Überblick über DNS-Anfragen auf **X4100/200/300** zu ermöglichen.

DNS-Proxy

Der DNS-Proxy macht das umständliche Pflegen von HOSTS-Dateien auf Rechnern im LAN überflüssig, da Sie **X4100/200/300** als DNS-Server auf den entsprechenden Rechnern eintragen können. DNS-Anfragen werden vom Rechner an **X4100/200/300** weitergeleitet und dort bearbeitet. Dadurch gestaltet sich die Konfiguration der Rechner im LAN einfach und kann auch bei Provider-Veränderungen belassen werden. Dies funktioniert auch, wenn die Rechner im LAN keine statischen DNS-Servereinträge haben, sondern diese dynamisch von **X4100/200/300** als DHCP-Server zugewiesen bekommen.

Durch Forwarding-Einträge kann **X4100/200/300** entscheiden, welcher DNS-Server zur Auflösung bestimmter Namen herangezogen werden soll. Wenn Sie also z. B. auf **X4100/200/300** zwei WAN-Partner konfiguriert haben, Ihre Firmenzentrale und Ihren Internet Service Provider, ist es sinnvoll, Internet-Namen vom DNS-Server Ihres ISPs, Namen des Firmennetzes aber vom DNS-Server der Firmenzentrale auflösen zu lassen. Eine DNS-Anfrage zur Auflösung einer internen Firmenadresse kann vom DNS-Server des ISPs in der Regel nicht beantwortet werden und ist somit überflüssig, verursacht unnötige Kosten und die Auflösung dauert länger als nötig. Somit ist ein Forwarding-Eintrag sinnvoll, der DNS-Anfragen nach Namen wie "*.intranet.de", an den WAN-Partner "Firmenzentrale" weiterleitet.

DNS-Cache

Wenn eine DNS-Anfrage von **X4100/200/300** an einen DNS-Server weitergeleitet und von diesem mit einem DNS-Record beantwortet wird, wird der so auf-

gelöste Name mit der zugehörigen IP-Adresse als positiver dynamischer Eintrag im DNS-Cache auf **X4100/200/300** gespeichert. Wenn also ein einmal aufgelöster Name erneut benötigt wird, kann **X4100/200/300** die Anfrage aus dem Cache beantworten, eine Anfrage an einen externen Name-Server ist nicht erneut nötig. Damit können diese Anfragen schneller beantwortet werden, Bandbreite auf den WAN-Verbindungen und Kosten für unnötige Verbindungen werden eingespart.

Wenn eine DNS-Anfrage von keinem der befragten DNS-Server beantwortet werden kann, wird dies im Cache als negativer dynamischer Eintrag gespeichert. Da fehlgeschlagene, also nicht zu beantwortende, DNS-Anfragen in der Regel von Applikationen oder IP-Stacks nicht gespeichert werden, können diese im Cache gespeicherten negativen dynamischen Einträge häufige, erfolglose Verbindungsaufbauten zu externen DNS-Servern verhindern.

Die Gültigkeit der positiven dynamischen Einträge im Cache ergibt sich aus der TTL (Time To Live), die im DNS-Record enthalten ist. Negativen Einträgen wird der Wert **Maximum TTL for Neg Cache Entries** zugewiesen. Nach Ablaufen der TTL wird ein dynamischer Eintrag aus dem Cache gelöscht.

Statische Namenseinträge

Mit positiven statischen Einträgen geben Sie auf **X4100/200/300** Namen mit den dazugehörigen IP-Adressen ein. Wenn Sie auf diese Weise häufig benötigte IP-Adressen speichern, kann **X4100/200/300** entsprechende DNS-Anfragen selbst beantworten, die Verbindung zu einem externen Name-Server ist nicht nötig. Damit wird der Zugriff auf diese Adressen beschleunigt. Für ein kleines Netzwerk kann so ein Name-Server auf **X4100/200/300** eingerichtet werden, die Installation eines separaten DNS-Servers bzw. die umständliche Pflege von HOSTS-Dateien auf den Rechnern im LAN ist nicht erforderlich.

Bei negativen statischen Einträgen wird einem Namen keine IP-Adresse zugeordnet, eine entsprechende DNS-Anfrage wird negativ beantwortet und auch an keinen anderen Name-Server weitergeleitet.

Einen dynamischen Eintrag können Sie in ***IP*** ➧ ***DNS*** ➧ ***DYNAMIC CACHE*** in einen statischen umwandeln (siehe Tabelle 7-43, Seite 251).

Filterfunktion

Durch Verwendung von negativen statischen Einträgen können Sie die Namensauflösung auf **X4100/200/300** durch eine Filterfunktion einschränken. Der

Zugriff auf bestimmte Domains kann so für Benutzer im LAN wesentlich erschwert werden, da verhindert wird, daß die entsprechenden Namen aufgelöst werden. Bei der Eingabe des Namens können Sie Wildcards (*) verwenden.

Bei Eingeben eines statischen Eintrags legen Sie fest, wie lange die dadurch vorgenommene Zuordnung von Name und IP-Adresse gültig ist, indem Sie die TTL vorgeben. Diese TTL wird in jeden DNS-Record eingetragen, mit dem **X4100/200/300** auf eine entsprechende DNS-Anfrage antwortet.

Achten Sie bei Ihren statischen Einträgen darauf, daß diese immer auf dem aktuellen Stand sind. Änderungen von Namen oder IP-Adressen können hin und wieder vorkommen!

Monitorfunktion

Welche IP-Adressen werden wie oft von Hosts im LAN angefordert?

Mit dem Setup Tool ist ein schneller Zugriff auf diese und andere statistische Informationen möglich. Mit dem Kommando `nslookup` in der Kommandozeile (SNMP-Shell) können Sie zudem prüfen, wie ein Name oder eine IP-Adresse durch **X4100/200/300** oder durch einen anderen Name-Server aufgelöst wird (siehe Kapitel 13.1, Seite 418). Hilfe zu dem Kommando erhalten Sie durch Eingabe von `nslookup -?`.

Weitere Möglichkeiten

Globale Name-Server

Desweiteren können Sie unter ***IP*** ➧ ***STATIC SETTINGS*** die IP-Adresse von globalen Name-Servern eintragen, die bevorzugt befragt werden sollen, wenn **X4100/200/300** Anfragen nicht selbst oder durch Forwarding-Einträge beantworten kann.

Für lokale Anwendungen kann als globaler Name-Server die IP-Adresse von **X4100/200/300** oder die Loopback-Adresse (127.0.0.1) eingetragen werden.

Die Adressen von Name-Servern kann **X4100/200/300** gegebenenfalls an WAN-Partner übermitteln bzw. von WAN-Partnern erhalten:

Default Interface

Zudem können Sie unter **Default Interface** einen WAN-Partner auswählen, zu dem dann für eine Name-Server-Verhandlung eine Verbindung aufgebaut wird, wenn eine Namensauflösung durch die bereits genannten Methoden nicht erfolgreich war.

Austausch von DNS-Server-Adressen mit LAN-Partnern

DHCP

Wenn **X4100/200/300** als DHCP-Server konfiguriert ist, können den DHCP-Clients im LAN IP-Adressen von Name-Servern übermittelt werden. Dabei können die Adressen der auf **X4100/200/300** eingetragenen globalen Name-Server übermittelt werden oder die Adresse von **X4100/200/300** selbst. Im letzteren Fall gehen DNS-Anfragen von den DHCP-Clients an **X4100/200/300**, der diese entweder selbst beantwortet oder gegebenenfalls weiterleitet (Proxy-Funktion).

Austausch von DNS-Server-Adressen mit WAN-Partnern

IP Control Protocol (IPCP)

Das gleiche gilt, wenn bei der IP-Konfiguration eines WAN-Partners die dynamische Aushandlung von Name-Servern aktiviert ist und **X4100/200/300** im Servermodus arbeitet (**Dynamic Name Server Negotiation** = *server (send)*). In diesem Fall können bei Name-Server-Verhandlungen über IPCP mit dem WAN-Partner, der IP-Address-Client ist, ebenfalls die Adressen der globalen Name-Server oder die Adresse von **X4100/200/300** selbst übermittelt werden.

Wenn **X4100/200/300** im Client-Modus arbeitet (**Dynamic Name Server Negotiation** = *client (receive)*), können gegebenenfalls Name-Server-Adressen mit dem WAN-Partner, der IP-Address-Server ist, ausgehandelt und an **X4100/200/300** übermittelt werden. Diese können als globale Name-Server auf **X4100/200/300** eingetragen werden und somit für zukünftige Namensauflösungen zur Verfügung stehen.

Strategie zur Namensauflösung auf X4100/200/300

Eine DNS-Anfrage wird von **X4100/200/300** folgendermaßen behandelt:

1. Kann die Anfrage aus dem statischen oder dynamischen Cache direkt beantwortet werden (IP-Adresse oder negative Antwort)?
   - Falls ja, wird die Information weitergeleitet.
   - Falls nein, siehe 2.
2. Ist ein passender Forwarding-Eintrag vorhanden?
   In diesem Fall werden die entsprechenden DNS-Server befragt. Falls die Verbindung zum WAN-Partner nicht aktiv ist, wird versucht, sie aufzubauen.
   - Falls ein DNS-Server den Namen auflösen kann, wird die Information weitergeleitet und ein dynamischer Eintrag im Cache erzeugt.

- Falls keiner der befragten DNS-Server den Namen auflösen kann oder kein passender Forwarding-Eintrag vorhanden ist, siehe 3.

3. Sind globale Name-Server eingetragen?
   In diesem Fall werden die entsprechenden DNS-Server befragt. Ist für lokale Anwendungen die IP-Adresse von **X4100/200/300** oder die Loopback-Adresse eingetragen, werden diese hier ignoriert.
   - Falls ein DNS-Server den Namen auflösen kann, wird die Information weitergeleitet und ein dynamischer Eintrag im Cache erzeugt.
   - Falls keiner der befragten DNS-Server den Namen auflösen kann oder keine statischen Name-Server eingetragen sind, siehe 4.
4. Ist ein WAN-Partner als Default Interface ausgewählt?
   In diesem Fall werden die dazugehörigen DNS-Server befragt. Falls die Verbindung zum WAN-Partner nicht aktiv ist, wird versucht, sie aufzubauen.
   - Falls ein DNS-Server den Namen auflösen kann, wird die Information weitergeleitet und ein dynamischer Eintrag im Cache erzeugt.
   - Falls keiner der befragten DNS-Server den Namen auflösen kann oder kein Default Interface ausgewählt wurde, siehe 5.
5. Ist das Überschreiben der Adressen der globalen Name-Server zulässig (**Overwrite Global Nameserver** = *yes*)?
   In diesem Fall wird eine Verbindung zum ersten WAN-Partner aufgebaut, der so konfiguriert ist, daß Adressen von DNS-Servern übermittelt werden könnten – soweit dies vorher noch nicht versucht wurde. Bei erfolgreicher Name-Server-Aushandlung werden diese als globale Name-Server eingetragen und stehen somit für weitere Anfragen zur Verfügung.
6. Anfrage wird mit Serverfehler beantwortet.

Wenn einer der DNS-Server mit "non-existent domain" antwortet, wird diese Antwort sofort an die Quelle der Anfrage weitergeleitet und in den Cache als Negativ-Eintrag aufgenommen.

Konfiguration mit Setup Tool – Überblick

Die Konfiguration und Überwachung der Namensauflösung auf **X4100/200/300** erfolgt in den Menüs:

- ***IP*** ➧ ***STATIC SETTINGS***:
- ***IP*** ➧ ***DNS***
- ***IP*** ➧ ***DNS*** ➧ ***STATIC HOSTS***
- ***IP*** ➧ ***DNS*** ➧ ***FORWARDED DOMAINS***
- ***IP*** ➧ ***DNS*** ➧ ***DYNAMIC CACHE***
- ***IP*** ➧ ***DNS*** ➧ ***ADVANCED SETTINGS...***
- ***IP*** ➧ ***DNS*** ➧ ***GLOBAL STATISTICS...***
- ***WAN PARTNER*** ➧ ***EDIT*** ➧ ***IP*** ➧ ***ADVANCED SETTINGS***

Das Menü ***IP*** ➧ ***STATIC SETTINGS*** enthält folgende Felder:

Feld	Bedeutung
Domain Name	Legt **X4100/200/300**s Domain Name fest.
Primary Domain Name Server	IP-Adresse von **X4100/200/300**s erstem globalen Domain-Name-Server (DNS).
Secondary Domain Name Server	IP-Adresse eines weiteren globalen Domain-Name-Servers.
Primary WINS	IP-Adresse von **X4100/200/300**s erstem globalen WINS (Windows Internet Name Server) bzw. NBNS (NetBIOS Name Server).
Secondary WINS	IP-Adresse eines weiteren globalen WINS bzw. NBNS.

Tabelle 7-39: ***IP*** ➧ ***STATIC SETTINGS***

Das Menü ***IP*** ➧ ***DNS*** enthält folgende Felder:

Feld	Bedeutung
Positive Cache	Ermöglicht positive dynamische Einträge im Cache. Mögliche Werte: ■ *enabled* (Standardwert): Erfolgreich aufgelöste Namen und IP-Adressen werden im Cache gespeichert. ■ *flush*: Alle positiven dynamischen Einträge im Cache werden gelöscht. ■ *disabled*: Erfolgreich aufgelöste Namen und IP-Adressen werden nicht im Cache gespeichert, bereits vorhandene dynamische positive Einträge werden gelöscht (statische Einträge werden nicht gelöscht).
Negative Cache	Ermöglicht negative dynamische Einträge im Cache. Mögliche Werte: ■ *enabled* (Standardwert): Namen, die nicht aufgelöst werden konnten, werden als negative Einträge im Cache gespeichert. ■ *flush*: Alle negativen dynamischen Einträge im Cache werden gelöscht. ■ *disabled*: Namen, die nicht aufgelöst werden konnten, werden nicht im Cache gespeichert, bereits vorhandene dynamische negative Einträge werden gelöscht (statische Einträge werden nicht gelöscht).

Feld	Bedeutung
Overwrite Global Nameservers	Legt fest, ob die Adressen von globalen Name-Servern auf **X4100/200/300** (in ***IP*** ➧ ***STATIC SETTINGS***) mit von WAN-Partnern übermittelten Name-Server-Adressen überschrieben werden dürfen. Mögliche Werte: ■ *yes* (Standardwert) ■ *no*
Default Interface	Legt den WAN-Partner fest, zu dem dann eine Verbindung zur Name-Server-Verhandlung aufgebaut wird, wenn andere Versuche zur Namensauflösung nicht erfolgreich waren.
DHCP Assignment	Legt fest, welche Name-Server-Adressen dem DHCP-Client übermittelt werden, wenn **X4100/200/300** als DHCP-Server konfiguriert ist. Mögliche Werte: ■ *none*: Es wird keine Name-Server-Adresse übermittelt. ■ *self* (Standardwert): Es wird die Adresse von **X4100/200/300** als Name-Server-Adresse übermittelt. ■ *global*: Es werden die Adressen der auf **X4100/200/300** eingetragenen globalen Name-Server übermittelt.

Feld	Bedeutung
IPCP Assignment	Legt fest, welche Name-Server-Adressen von **X4100/200/300** bei einer dynamischen Name-Server-Verhandlung an einen WAN-Partner übermittelt werden. Mögliche Werte: ■ *none*: Es wird keine Name-Server-Adresse übermittelt. ■ *self*: Es wird die Adresse von **X4100/200/300** als Name-Server-Adresse übermittelt. ■ *global* (Standardwert): Es werden die Adressen der auf **X4100/200/300** eingetragenen globalen Name-Server übermittelt.
Static Hosts	In Klammern wird die Anzahl der statischen Einträge angezeigt.
Forwarded Domains	In Klammern wird die Anzahl der Forwarding-Einträge angezeigt.
Dynamic Cache	In Klammern wird die Anzahl der positiven und negativen dynamischen Einträge im DNS-Cache angezeigt.

Tabelle 7-40: ***IP*** ➧ ***DNS***

Das Menü ***IP*** ➧ ***DNS*** ➧ ***STATIC HOSTS*** ➧ ***ADD*** enthält folgende Felder:

Feld	Bedeutung
Default Domain:	Der in ***IP*** ➧ ***STATIC SETTINGS*** eingetragene Domain Name von **X4100/200/300** wird angezeigt.

Feld	Bedeutung
Name	Host-Name, dem **Address** mit diesem statischen Eintrag zugeordnet wird. Kann auch Wildcards (*) enthalten (nur am Anfang von **Name**, z. B. *.bintec.de). Bei Eingabe eines unvollständigen Namens ohne Punkt wird dieser nach Bestätigung mit **SAVE** mit ".**Default Domain**" vervollständigt.
Response	Legt fest, welcher Art der statische Eintrag ist. Mögliche Werte: ■ *positive* (Standardwert): Ein DNS-Request nach **Name** wird mit einem DNS-Record beantwortet, der die dazugehörige **Address** enthält. ■ *ignore*: Ein DNS-Request wird ignoriert, es wird keine Antwort gegeben (auch keine negative). ■ *negative*: Ein DNS-Request nach **Name** wird mit einer negativen Antwort beantwortet.
Address	(nur bei **Response** = *positive*) IP-Adresse, die **Name** zugeordnet wird.
TTL	Gültigkeitsdauer der Zuordnung von **Name** zu **Address** in Sekunden (nur relevant bei **Response** = *positive*). Dieser Wert wird dem TTL-Feld (Time To Live) gegeben, falls **X4100/200/300** einen entsprechenden DNS-Record verschickt. Standardwert: *86400* (= 24 h)

Tabelle 7-41: ***IP*** ➧ ***DNS*** ➧ ***STATIC HOSTS*** ➧ ***ADD***

Das Menü ***IP*** ➧ ***DNS*** ➧ ***FORWARDED DOMAINS*** ➧ ***ADD*** enthält folgende Felder:

Feld	Bedeutung
Global Nameservers:	Die in ***IP*** ➧ ***STATIC SETTINGS*** eingetragenen globalen Name-Server werden angezeigt.
Default Domain:	Der in ***IP*** ➧ ***STATIC SETTINGS*** eingetragene Domain Name von **X4100/200/300** wird angezeigt.
Name	Host-Name, der mit diesem Forwarding-Eintrag aufgelöst werden soll. Kann auch Wildcards enthalten (nur am Anfang von **Name**, z. B. *.bintec.de). Bei Eingabe eines unvollständigen Namens ohne Punkt wird dieser nach Bestätigung mit **SAVE** mit ".**Default Domain**" vervollständigt.
Interface	Legt den WAN-Partner fest, zu dem zur Auflösung von **Name** eine Verbindung aufgebaut wird.
TTL	Gültigkeitsdauer der Zuordnung von **Name** zu **Address** in s. Standardwert: *86400* (= 24 h) Wenn die Anfrage von **X4100/200/300** nach **Name** mit einem DNS-Record beantwortet wird, enthält dieser ein TTL-Feld (= Time To Live in Sekunden), dessen Wert bei Weiterleiten des DNS-Records von **X4100/200/300** in der Regel nicht verändert wird. Falls das erhaltene TTL-Feld den Wert 0 hat oder **Maximum TTL for Pos Cache entries** überschreitet, wird dem weitergeleiteten DNS-Record **TTL** mitgegeben.

Tabelle 7-42: ***IP*** ➧ ***DNS*** ➧ ***FORWARDED DOMAINS*** ➧ ***ADD***

Das Menü ***IP*** ➧ ***DNS*** ➧ ***DYNAMIC CACHE*** enthält folgende Felder:

Feld	Bedeutung
Name	Host-Name, dem **Address** mit diesem dynamischen Eintrag im Cache zugeordnet wird.
Address	IP-Adresse, die **Name** zugeordnet wird.
Resp	Legt fest, welcher Art der dynamische Eintrag ist. Mögliche Werte: ■ *positive*: Ein DNS-Request nach **Name** wird aus dem Cache mit der dazugehörigen IP-Addresse beantwortet. ■ *negative*: Ein DNS-Request nach **Name** wird aus dem Cache mit einer negativen Antwort beantwortet.
TTL	Gibt an, wie viele Sekunden der dynamische Eintrag noch im Cache bleibt. Nach Ablauf von **TTL** wird der Eintrag gelöscht. Bei Speicherung eines positiven dynamischen Eintrags im Cache wird hier der Wert des im DNS-Record enthaltenen TTL-Felds (= Time To Live in Sekunden) übernommen. Wenn das TTL-Feld im DNS-Record auf 0 gesetzt ist oder **Maximum TTL for Pos Cache entries** überschreitet, wird hier bei Speicherung des Eintrags der Wert **Maximum TTL for Pos Cache entries** vergeben. Bei Speicherung eines negativen dynamischen Eintrags im Cache wird hier immer **Maximum TTL for Neg Cache entries** vergeben.
Ref	Gibt an, wie oft der Eintrag referenziert wurde, also wie oft ein DNS-Request mit dem Eintrag aus dem Cache beantwortet wurde.

Feld	Bedeutung
STATIC	Durch Markieren eines Eintrags mit der **Leertaste** und bestätigen mit STATIC wird ein dynamischer Eintrag in einen statischen umgewandelt. Der entsprechende Eintrag verschwindet damit aus ***IP*** ➧ ***DNS*** ➧ ***DYNAMIC CACHE*** und wird in ***IP*** ➧ ***DNS*** ➧ ***STATIC HOSTS*** aufgelistet. **TTL** wird dabei übernommen.

Tabelle 7-43: ***IP*** ➧ ***DNS*** ➧ ***DYNAMIC CACHE***

Das Menü ***IP*** ➧ ***DNS*** ➧ ***ADVANCED SETTINGS...*** enthält folgende Felder:

Feld	Bedeutung
Maximum Number of DNS Records	Legt die maximale Anzahl der statischen und dynamischen Einträge fest. Ist dieser Wert erreicht, wird bei einem neu hinzukommenden Eintrag ein älterer dynamischer Eintrag aus dem Cache gelöscht. Dabei wird jeweils der dynamische Eintrag gelöscht, nach dem am längsten nicht mehr gefragt wurde. Wird **Maximum Number of DNS Records** vom Benutzer heruntergesetzt, werden gegebenenfalls dynamische Einträge gelöscht. Statische Einträge werden nicht gelöscht, **Maximum Number of DNS Records** kann nicht kleiner als die aktuell vorhandene Anzahl von statischen Einträgen gesetzt werden. Entspricht **Maximum Number of DNS Records** der Anzahl der statischen Einträge, sind keine weiteren dynamischen Einträge möglich!
Maximum TTL for Pos Cache entries	Wird einem positiven dynamischen Eintrag im Cache als **TTL** vergeben, wenn das TTL-Feld des erhaltenen DNS-Records den Wert 0 hat oder **Maximum TTL for Pos Cache entries** überschreitet.

Feld	Bedeutung
Maximum TTL for Neg Cache Entries	Wird einem negativen dynamischen Eintrag im Cache als **TTL** vergeben.

Tabelle 7-44: ***IP*** ➧ ***DNS*** ➧ ***ADVANCED SETTINGS...***

Das Menü ***IP*** ➧ ***DNS*** ➧ ***GLOBALS STATISTICS...*** enthält folgende Felder (das Menü wird jede Sekunde aktualisiert):

Feld	Bedeutung
Received DNS Packets	Zeigt die Anzahl der empfangenen DNS-Pakete an, einschließlich der Antwortpakete auf weitergeleitete Anfragen.
Invalid DNS Packets	Zeigt die Anzahl der empfangenen ungültigen DNS-Pakete an.
DNS Requests	Zeigt die Anzahl der korrekt empfangenen DNS-Requests an.
Cache Hits	Zeigt die Anzahl der Anfragen an, die mit statischen oder dynamischen Einträgen aus dem Cache beantwortet werden konnten.
Forwarded Requests	Zeigt die Anzahl der Anfragen an, die an andere Name-Server weitergeleitet wurden.
Cache Hitrate (%)	Zeigt die Anzahl von **Cache Hits** pro **DNS Requests** in Prozent an.
Successfully Answered Queries	Zeigt die Anzahl der erfolgreich (positiv und negativ) beantworteten Anfragen an.
Server Failures	Zeigt die Anzahl der Anfragen an, die kein Name-Server (weder positiv noch negativ) beantworten konnte.

Tabelle 7-45: ***IP*** ➧ ***DNS*** ➧ ***GLOBALS STATISTICS...***

Folgendes Feld von ***WAN PARTNER*** ➧ ***EDIT*** ➧ ***IP*** ➧ ***ADVANCED SETTINGS*** ist für diesen Konfigurationsschritt relevant:

Feld	Bedeutung
Dynamic Name Server Negotiation	Legt fest, ob **X4100/200/300** IP-Adressen für **Primary Domain Name Server**, **Secondary Domain Name Server**, **Primary WINS** und **Secondary WINS** im Falle einer dynamischen Name-Server-Aushandlung vom WAN-Partner erhält oder an den WAN-Partner sendet.

Tabelle 7-46: ***WAN PARTNER*** ➧ ***EDIT*** ➧ ***IP*** ➧ ***ADVANCED SETTINGS***

Das Feld **Dynamic Name Server Negotiation** enthält folgende Auswahlmöglichkeiten:

Mögliche Werte	Bedeutung
off	**X4100/200/300** sendet und beantwortet keine Anfragen nach Name-Server-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**: ■ **X4100/200/300** sendet Anfragen nach Name-Server-Adressen an den WAN-Partner, falls *dynamic client* ausgewählt ist. ■ **X4100/200/300** beantwortet Anfragen des WAN-Partners nach Name-Server-Adressen, falls *dynamic server* ausgewählt ist. ■ **X4100/200/300** beantwortet, aber sendet keine Anfragen nach Name-Server-Adressen, falls *yes* oder *no* ausgewählt ist.
client (receive)	**X4100/200/300** sendet Anfragen nach Name-Server-Adressen an den WAN-Partner.

Mögliche Werte	Bedeutung
server (send)	**X4100/200/300** beantwortet Anfragen des WAN-Partners nach Name-Server-Adressen.

Tabelle 7-47: **Dynamic Name Server Negotiation**

Konfiguration mit dem Setup Tool – Vorgehensweise

Namensauflösung auf X4100/200/300

Im folgenden wird erklärt, wie Sie Namensauflösung mit dem DNS-Proxy auf **X4100/200/300** konfigurieren.

ToDo

Tragen Sie gegebenenfalls zunächst globale Name-Server auf **X4100/200/300** ein:

- Gehen Sie zu ***IP*** ➧ ***STATIC SETTINGS***.
- Geben Sie **Domain Name** ein, z. B. ***mycompany.com***.
- Geben Sie gegebenenfalls **Primary** bzw. **Secondary Domain Name Server** ein.
- Geben Sie gegebenenfalls **Primary** bzw. **Secondary WINS** ein.

Wenn Sie keinen Secondary DNS bzw. Secondary WINS Server haben, können Sie ein zweites Mal die IP-Adresse des Primary DNS bzw. WINS Servers in das Feld **Secondary Domain Name Server** bzw. **Secondary WINS** eingeben.

Dies kann für die Verbindung mit manchen DFÜ-Clients notwendig sein.

- Bestätigen Sie mit **SAVE**.

Aktivieren bzw. deaktivieren Sie die Cache-Funktion und legen Sie allgemeine Einstellungen für den DNS-Proxy fest:

- Gehen Sie zu ***IP*** ➧ ***DNS***.
- Wählen Sie **Positive Cache** und **Negative Cache** aus, z. B. ***enabled***.
- Wählen Sie **Overwrite Global Nameservers** aus, z. B. ***yes***, wenn Sie unter ***IP*** ➧ ***STATIC SETTINGS*** keine globalen Name-Server statisch eintragen wollen.
- Wählen Sie **DHCP Assignment** aus, z. B. ***self***.

- Wählen Sie **IPCP Assignment** aus, z. B. ***global***.

Legen Sie die Werte für die statischen und dynamischen Einträge fest:

- Gehen Sie zu ***IP*** ➧ ***DNS*** ➧ ***ADVANCED SETTINGS...***.
- Tragen Sie **Maximum Number of DNS Records** ein.
- Tragen Sie **Maximum TTL for Pos Cache entries** ein.
- Tragen Sie **Maximum TTL for Neg Cache Entries** ein.
- Bestätigen Sie mit **SAVE**.

So erzeugen Sie statische Einträge:

- Gehen Sie zu ***IP*** ➧ ***DNS*** ➧ ***STATIC HOSTS***.
  Hier sind alle vorhandenen statischen Einträge aufgelistet.
- Mit **ADD** erzeugen Sie einen neuen Eintrag.
- Geben Sie **Name** ein.
- Wählen Sie **Response** aus.
- Geben Sie gegebenenfalls **Address** ein.
- Geben Sie **TTL** ein.
- Bestätigen Sie mit **SAVE**.

So erzeugen Sie Forwarding-Einträge:

- Gehen Sie zu ***IP*** ➧ ***DNS*** ➧ ***FORWARDED DOMAINS***.
  Hier sind alle vorhandenen Forwarding-Einträge aufgelistet.
- Mit **ADD** erzeugen Sie einen neuen Eintrag.
- Geben Sie **Name** ein.
- Wählen Sie **Interface** aus.
- Geben Sie **TTL** ein.
- Bestätigen Sie mit **SAVE**.
- Wählen Sie **EXIT**.
- Bestätigen Sie mit **SAVE**.

➤ Bestätigen Sie mit **EXIT**.

Sie befinden sich wieder im Hauptmenü. Die Eintragungen sind temporär gespeichert und aktiviert.

DNS-Aushandlung aktivieren

Wenn Sie einen WAN-Partner so konfigurieren möchten, daß die Adresse eines Name-Servers gegebenenfalls von **X4100/200/300** an den WAN-Partner oder vom WAN-Partner an **X4100/200/300** übermittelt wird, gehen Sie folgendermaßen vor:

➤ Gehen Sie zu ***WAN PARTNER*** ➧ ***EDIT*** ➧ ***IP*** ➧ ***ADVANCED SETTINGS***.

➤ Wählen Sie die gewünschte Funktion für **Dynamic Name Server Negotiation** aus.

➤ Bestätigen Sie mit **OK**.

➤ Bestätigen Sie mit **SAVE**.

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

Monitoring und Statistik

So verschaffen Sie sich einen Überblick über dynamische Einträge im Cache:

➤ Gehen Sie zu ***IP*** ➧ ***DNS*** ➧ ***DYNAMIC CACHE***.

Hier sind alle im Cache vorhandenen dynamischen Einträge aufgelistet.

➤ Um einen dynamischen in einen statischen Eintrag umzuwandeln, markieren Sie den Eintrag mit der **Space**-Taste und bestätigen Sie mit **STATIC**.

Der Eintrag verschwindet aus der Liste der dynamischen Einträge und wird unter ***IP*** ➧ ***DNS*** ➧ ***STATIC HOSTS*** als statischer Eintrag aufgelistet.

So verschaffen Sie sich einen Überblick über einige statistische Werte:

➤ Gehen Sie zu ***IP*** ➧ ***DNS*** ➧ ***GLOBAL STATISTICS...***.

Hier finden Sie einiges an Statistik zum DNS-Proxy.

7.3.3 Port-Nummern

Was ist ein ➤➤ Port?

X4100/200/300 verfügt über mehrere Dienste bzw. Anwendungen, z. B. SNMP, ➤➤ **Telnet**. 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 **X4100/200/300** neben der IP-Adresse

auch einen Port an. So wird der entsprechende Dienst angesprochen. Ports gibt es nur bei den Protokollen TCP und UDP!

X4100/200/300 leitet eingehende ➤➤ **Datenpakete** an den Port mit der zur gewünschten Applikation gehörigen Nummer weiter. Damit wird die entsprechende Applikation von **X4100/200/300** angesprochen, die eingehenden Daten können verarbeitet werden.

Gewöhnlich sind die Voreinstellungen zutreffend. Nehmen Sie hier also nur Änderungen vor, wenn dies nötig ist.

In ***IP*** ➧ ***STATIC SETTINGS*** können Sie einige wichtige Port-Nummern festlegen:

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.

Tabelle 7-48: ***IP*** ➧ ***STATIC SETTINGS***

ToDo Gehen Sie folgendermaßen vor, wenn Sie eine der Port-Nummern verändern wollen:

➤ Gehen Sie zu ***IP*** ➧ ***STATIC SETTINGS.***

➤ Geben Sie **Remote CAPI Server TCP port**, **Remote TRACE Server TCP port** und **RIP UDP port** ein.

➤ Bestätigen Sie mit **SAVE**.

Die Port-Nummern sind geändert.

7.3.4 BOOTP-Relay-Agent

Bootstrap Protocol

Das Bootstrap-Protokoll (➤➤ **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.

Hier eine grafische Darstellung:

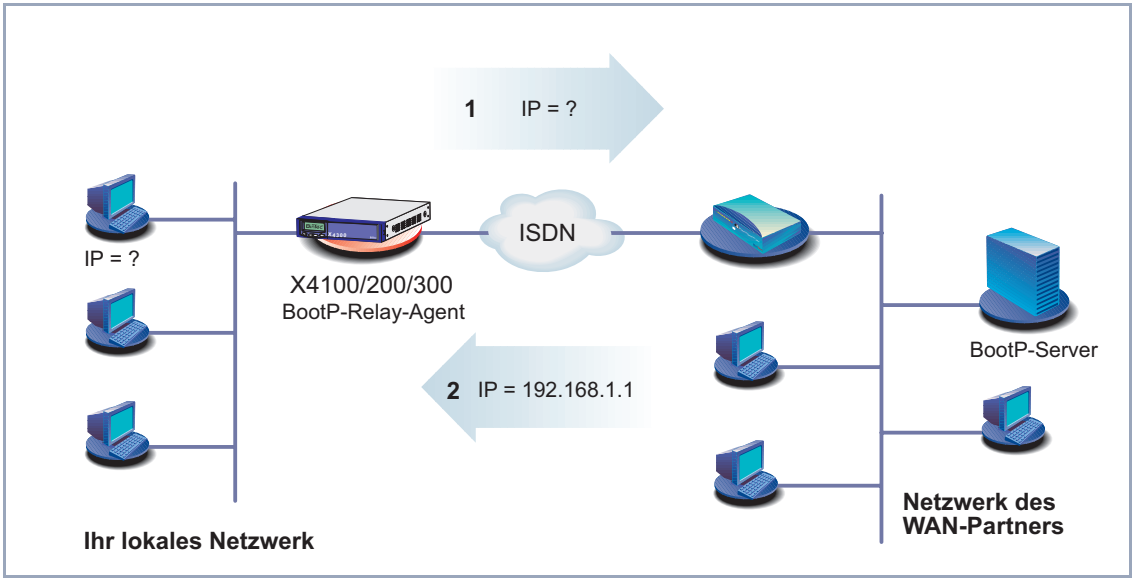


Bild 7-4: **X4100/200/300** als BOOTP-Relay-Agent

Die Konfiguration erfolgt in ***IP*** ➧ ***STATIC SETTINGS***:

Feld	Bedeutung
BOOTP Relay Server	IP-Adresse des BOOTP-Servers.

Tabelle 7-49: ***IP*** ➧ ***STATIC SETTINGS***

ToDo Gehen Sie folgendermaßen vor:

Wenn für die Verbindung zwischen BOOTP-Server und BOOTP-Client eine WAN-Verbindung erforderlich ist, muß ein entsprechender WAN-Partner eingerichtet sein (siehe Kapitel 6.3, Seite 147).

- Gehen Sie zu ***IP*** ➧ ***STATIC SETTINGS***.
- Geben Sie die IP-Adresse von **BOOTP Relay Server** ein.
- Bestätigen Sie mit **SAVE**.

  X4100/200/300 ist als BOOTP-Relay-Agent konfiguriert.

7.4 Quality of Service (QoS)

Was ist QoS?

Gestiegene Internet- und Intranetbelastung sowie die Tendenz zu konvergierenden Sprachdatennetzen erzwingt ein intelligentes Bandbreitenmanagement. Mit "Quality of Service" werden vorhandene Bandbreiten intelligent und effektiv kontrolliert, ggf. reserviert und den unterschiedlichen Diensten zugeteilt. Dabei geht es um:

- Vermeidung von Überlastsituationen in Netzwerksegmenten und WAN-Strecken
- Minimierung der Verluste von IP-Paketen
- Optimierung der Verzögerung (Latenzzeit) für bestimmte Dienste

Um IP-QoS zu realisieren, sollten Sie grundsätzlich einem dreistufigen Prozeß folgen: Identifizieren Sie zunächst die Datenströme in Ihren Netzwerksegmenten und quantifizieren Sie, um dann entsprechend den Anforderungen bestimmter Applikationen Bandbreiten zuweisen und Nutzer priorisieren zu können.

QoS bei BinTec

Mit der Funktion "Quality of Service" bietet **X4100/200/300** QoS-Unterstützung für die IP-Protokollfamilie. Die QoS-Behandlung erfolgt nach dem "Differentiated Services Model", d. h. auf Basis einer IP-Paket-Klassifizierung (Diensteerkennung). Mit der Klassifizierung werden – anhand eines Regelwerkes (siehe auch Kapitel 9.2.8, Seite 339) – die IP-Pakete bestimmter Dienste über IP-Filter spezifiziert und in Paketklassen aufgeteilt. Die Klassifizierung wird Interface-spezifisch vorgenommen und kann sowohl auf LAN- als auch auf WAN-Interfaces erfolgen. Die klassifizierten IP-Pakete werden priorisiert. Die Priorisierung anhand konfigurierbarer Strategien ("Policies") ist derzeit auf WAN-Interfaces beschränkt und wird ebenfalls jeweils auf ein Interface bezogen vorgenommen.

Durch Signalisierung auf Paketebene kann ein Router den benachbarten Geräten mitteilen, daß bestimmte Daten besonders behandelt werden sollen. Die Signalisierung erfolgt durch die Markierung zuvor spezifizierter IP-Pakete über das TOS-Feld im IP-Header. QoS-Signalisierung ist nützlich, um den durch QoS-Funktionen bestimmten Datenverkehr zu koordinieren. Die erfolgreiche

Konfiguration eines netzwerkweiten QoS-Dienstes "end-to-end" hängt wesentlich von der Signalisierung ab.

Vorteile "Quality of Service" bietet folgende Vorteile:

- Zeitkritische Daten (z. B. VoIP) über WAN-Interfaces können vorrangig ("high-priority" Klasse) behandelt werden. Ein spezieller Algorithmus verringert die Latenzzeit solcher Pakete auf vergleichweise langsamen PPP-Verbindungen (MLPPP Interleave, siehe "Multilink PPP (MLPPP)", Seite 274).
- Datenströme können in bis zu 255 Unterklassen der normalen Prioritätsklasse aufgeteilt und differenziert behandelt werden.
- Es ist möglich, Bandbreite für bestimmte IP-Pakete (Dienste) zu reservieren ("Traffic Shaping").
- "Congestion Management": Überlastsituationen werden erkannt und über verschiedene Queueing-Algorithmen (PQ, WRR, WFQ, siehe "Algorithmen", Seite 271) aufgelöst.
- "Congestion Avoidance": Überlastsituationen (nur TCP-Flows) können durch "Random Early Detection" vermieden werden. Dadurch minimieren sich die Paketverluste insbesondere bei kurzzeitiger Überschreitung der zugelassenen Bandbreite (siehe "Congestion Avoidance", Seite 273).

Konfigurationsübersicht

Die Konfiguration erfolgt im Menü ***QoS***:

```
X4x00 Setup Tool                          BinTec Access Networks GmbH
[QoS]: QoS Configuration                                    MyRouter


                        IP Filter
                        IP Classification and Signalling

                        Interfaces and Policies



                        Exit

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

Um IP-QoS zu realisieren, sollten Sie grundsätzlich einem dreistufigen Prozeß folgen: Identifizieren Sie zunächst die Datenströme in Ihren Netzwerksegmenten und quantifizieren Sie, um dann entsprechend den Anforderungen bestimmter Applikationen oder Nutzer priorisieren zu können.

Im Untermenü ***QoS*** ➧ ***IP FILTER*** werden die IP-Filter definiert, um bestimmte IP-Pakete bzw. Dienste spezifizieren zu können. Die Vorgehensweise hierfür entspricht der für die Access-Listen, beschrieben in Kapitel 9.2.8, Seite 339.

Im Untermenü ***QoS*** ➧ ***IP CLASSIFICATION AND SIGNALLING*** erstellen Sie die Regelketten zur Klassifizierung der IP-Pakete anhand der zuvor definierten IP-Filter. Auf diese Weise können mehrere IP-Filter miteinander verknüpft und der Datenstrom in verschiedene Paketklassen eingeteilt werden. Es lassen sich damit aber auch völlig verschiedene Typen von IP-Paketen in einer Paketklasse zusammenfassen, die dann mit gleicher Priorität behandelt werden. Die Signalisierung für andere Netzwerkkomponenten (z. B. Switches) über das TOS-Feld wird ebenfalls über diese Regelketten definiert.

Im Untermenü ***QoS*** ➧ ***INTERFACES AND POLICIES*** legen Sie fest, auf welchem Interface mit welcher Regelkette klassifiziert werden soll. Auf dem Ethernet (en1) könnten z. B. alle eingehenden Pakete, auf einer WAN-Verbindung z. B. alle ausgehenden Pakete untersucht und klassifiziert werden.

Außerdem können Sie für ein oder mehrere WAN-Interfaces folgende Einstellungen vornehmen:

- Queueing-Strategie (PQ, WRR, WFQ usw.) im Menü ***QoS*** ➧ ***INTERFACES AND POLICIES*** ➧ **EDIT** ➧ ***QoS SCHEDULING AND SHAPING***
- Bandbreitenbegrenzungen und -reservierungen im Menü ***QoS*** ➧ ***INTERFACES AND POLICIES*** ➧ **EDIT** ➧ ***CLASS-BASED QoS POLICIES*** ➧ **ADD**
- Congestion-Avoidance-Strategien wie RED im Menü ***QoS*** ➧ ***INTERFACES AND POLICIES*** ➧ **EDIT** ➧ ***CLASS-BASED QoS POLICIES*** ➧ **ADD**
- Derzeit nur auf Single-Link-Verbindungen (nicht bei Kanalbündelung) möglich: MLPPP-Interleave-Verfahren zur Verminderung der Latenzzeit von "high-priority"-Paketen auf langsamen WAN-Verbindungen im Menü ***QoS*** ➧ ***INTERFACES AND POLICIES*** ➧ **EDIT**

7.4.1 IP-Filter definieren

Gehen Sie folgendermaßen vor, um IP-Filter zu definieren:

Ausführliche Beschreibungen zum Definieren von Filtern finden Sie in Kapitel 9.2.8, Seite 339.

- Gehen Sie zu ***QoS*** ➧ ***IP FILTER*** ➧ **ADD**.
- Definieren Sie Filter, wie in "Filter", Seite 349 beschrieben.
- Fahren Sie fort mit Kapitel 7.4.2, Seite 263.

7.4.2 Klassifizierung und (TOS-)Signalisierung

Bei der Klassifizierung werden die zuvor durch Filter spezifizierten IP-Pakete entweder einer "high-priority" oder einer "normal" Klasse zugeordnet. Letztere kann nochmals mittels einer "Class ID" in bis zu 255 Unterklassen aufgeteilt werden. Für jede dieser Unterklassen kann dann (Interface-spezifisch) genau festgelegt werden, wie mit den Paketen insbesondere in einer Überlastsituation zu verfahren ist (Policy).

Für die TOS-Signalisierung kann eine maximale Paketrate definiert werden. Pakete, die zur Überschreitung dieser Rate führen würden, werden dann nicht manipuliert, aber in Überlastsituationen bevorzugt verworfen, sofern sie nicht der "high-priority" Paketklasse angehören.

Die Klassifizierung und (TOS-)Signalisierung wird im Menü ***QoS*** ➧ ***IP CLASSIFICATION AND SIGNALLING*** ➧ **ADD** bzw. ***QoS*** ➧ ***IP CLASSIFICATION AND SIGNALLING*** ➧ **EDIT** festgelegt:

```
X4x00 Setup Tool                                    BinTec Access Networks
GmbH
[QOS][CLASS][ADD]: Configure IP QoS Classification and Signalling MyRouter

        Index                1

        Filter               test
        Direction            incoming

        Action               classify M

        Classification>
        Signalling (TOS)>

        Insert behind Rule   NONE

                          SAVE                    CANCEL

Use <Space> to select
```

Die Felder des Menüs ***QoS*** ➧ ***IP CLASSIFICATION AND SIGNALLING***:

Feld	Bedeutung
Index	Kann nicht verändert werden. **X4100/200/300** 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, hinter welcher Regel die neue Regel eingefügt wird. Mit *none* beginnen Sie eine neue eigenständige Kette.
Filter	IP-Filter, das verwendet wird.

Feld	Bedeutung
Direction	Richtung der Datenpakete, die auf die Filterbedingungen überprüft werden, um abhängig davon die Regel anzuwenden. Mögliche Werte: ■ *incoming*: eingehende Datenpakete ■ *outgoing*: ausgehende Datenpakete ■ *both*: eingehende und ausgehende Datenpakete
Action	Legt fest, wie mit einem ausgefilterten Datenpaket verfahren wird (siehe auch Tabelle 7-51, Seite 266).
Classification	In diesem Untermenü werden den IP-Paketen, für welche die Filterbedingungen zutreffen, Klassifizierungen zugeordnet (siehe auch Tabelle 7-52, Seite 266).
Signalling (TOS)	In diesem Untermenü wird ggf. ein neuer Wert für das TOS-Feld der die IP-Pakete, auf welche die Filterbedingungen zutreffen, definiert. So wird im Netzwerk signalisiert, daß diese IP-Pakete besonders behandelt werden sollen (siehe auch Tabelle 7-53, Seite 267).
Next Rule	Erscheint nur, wenn eine bestehende Regel editiert wird. Legt fest, welche Regel als nächste angewendet wird.

Tabelle 7-50: ***QoS*** ➧ ***IP Classification and Signalling*** ➧ **ADD**

Das Feld **Action** enthält folgende Auswahlmöglichkeiten:

Mögliche Werte	Bedeutung
disable	Regel wird deaktiviert. Weiter mit nächster Regel, falls vorhanden.
classify M	IP-Paket klassifizieren, wenn das Filter paßt.

Mögliche Werte	Bedeutung
classify !M	IP-Paket klassifizieren, wenn das Filter nicht paßt.

Tabelle 7-51: **Action**

Das Untermenü ***QoS*** ➧ ***IP CLASSIFICATION AND SIGNALLING*** ➧ **EDIT/ADD** ➧ ***CLASSIFICATION*** enthält folgende Auswahlmöglichkeiten:

Feld	Bedeutung
Class Type	Definiert **Class Type** für die IP-Pakete, für welche die Filterbedingungen zutreffen. Auf **Class Type** wird von den "QoS Policies" referenziert. Mögliche Werte: ■ *normal* ■ *high priority*
Class ID	Nur einstellbar, wenn **Class Type** *normal* gewählt wurde. Mögliche Werte: *1* bis *255*.

Tabelle 7-52: ***CLASSIFICATION***

Das Untermenü ***QoS*** ➧ ***IP CLASSIFICATION AND SIGNALLING*** ➧ **EDIT/ADD** ➧ ***SIGNALLING (TOS)*** enthält folgende Auswahlmöglichkeiten:

Feld	Bedeutung
Set Type of Service (TOS) Field	Definiert für die IP-Pakete, für welche die Filterbedingungen zutreffen, einen neuen Wert für das TOS-Feld im IP-Header. Mögliche Werte: *0* bis *255*

Feld	Bedeutung
Specify TOS Set Rate Limitation	(optional) Aktiviert bzw. deaktiviert **Maximum Rate (Packets per Second)** und **Maximum Burst Size (Number of Packets)**. Mögliche Werte: ■ *no* ■ *yes*
Maximum Rate (Packets per Second)	Anzahl der zu manipulierenden Pakete pro Sekunde. Nur einstellbar, wenn **Specify TOS Set Rate Limitation** auf *yes* gesetzt ist. Mögliche Werte: *0* bis *65535*.
Maximum Burst Size (Number of Packets)	Definiert die maximale Anzahl der Pakete, deren TOS-Feld auch dann noch gesetzt werden darf, wenn die zuvor definierte maximale Paketrate erreicht wurde. Nur einstellbar, wenn **Specify TOS Set Rate Limitation** auf *yes* gesetzt ist. Mögliche Werte: *0* bis *65535*.

Tabelle 7-53: ***SIGNALLING (TOS)***

Klassifikationsregeln festlegen

Gehen Sie folgendermaßen vor, um Klassifikationsregeln für die QoS-Filter festzulegen:

➤ Gehen Sie zu ***QOS*** ➧ ***IP CLASSIFICATION AND SIGNALLING***.

➤ 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 den gewünschten Wert für **Direction** aus.

➤ Wählen Sie den gewünschten Wert für **Action** aus.

➤ Wählen Sie den gewünschten **Filter** aus.

Klassifikation

- Gehen Sie nur zu ***QoS*** ➧ ***IP Classification and Signalling*** ➧ **EDIT/ADD** ➧ ***Classification***.
- Wählen Sie den gewünschten Wert für **Class Type** aus.
- Geben Sie gegebenenfalls eine **Class ID** ein (nur für **Class Type** *normal*).
- Bestätigen Sie mit **OK**.

TOS-Signalisierung aktivieren

- Gehen Sie gegebenenfalls zu ***QoS*** ➧ ***IP Classification and Signalling*** ➧ **EDIT/ADD** ➧ ***Signalling (TOS)***, falls die TOS-Signalisierung konfiguriert werden soll.
- Geben Sie den gewünschten Wert für **Set Type of Service (TOS) Field** ein.
- Wählen Sie den gewünschten Wert für **Specify TOS Set Rate Limitation** aus.
- Geben Sie gegebenenfalls den gewünschten Wert für **Maximum Rate (Packets per Second)** ein.
- Geben Sie gegebenenfalls den gewünschten Wert für **Maximum Burst Size (Number of Packets)** ein.
- Bestätigen Sie mit **OK**.

  Sie befinden sich wieder im Menü ***QoS*** ➧ ***IP Classification and Signalling*** ➧ **ADD** bzw. ***QoS*** ➧ ***IP Classification and Signalling*** ➧ **EDIT**.
- Wählen Sie **Insert behind Rule aus**, wenn Sie eine neue Regel erstellen, die an eine bestehende Regel angehängt werden soll.
- Wählen Sie gegebenenfalls **Next Rule** aus.
- Bestätigen Sie mit **SAVE**.

  Sie befinden sich wieder im Menü ***QoS*** ➧ ***IP Classification and Signalling***.
- Wiederholen Sie diese Schritte, bis Sie alle gewünschten Regeln definiert haben.
- Fahren Sie fort mit Kapitel 7.4.3, Seite 269.

7.4.3 Aktivierung der Klassifizierung

Im Menü ***QoS*** ➧ ***Interfaces and Policies*** legen Sie fest, auf welchem Interface die zuvor festgelegte Klassifizierung erfolgen soll:

```
X4x00 Setup Tool                              BinTec Access Networks GmbH
[QoS][INTERFACES]: Enable IP QoS Classification and Policies  MyRouter

Interface    First Rule   First Filter     Scheduler    TxRate   Limit

call-bycall      no IP QoS classification
dialup1          no IP QoS classification
en1              no IP QoS classification
en1-snap         no IP QoS classification
en4              no IP QoS classification
en4-snap         no IP QoS classification


EXIT

Use <Space> to select
```

Es kann immer nur eine Regelkette pro Interface erstellt werden. Sollen also mehrere IP-Filter auf einem Interface angewandt werden, so müssen diese über eine Regelkette miteinander verbunden werden. Besondere Sorgfalt ist erforderlich, falls es Überschneidungen zwischen mehreren Filtern gibt (Schnitt- bzw. Untermengen). Hier muß beachtet werden, daß die Abarbeitung einer Regelkette für jedes IP-Paket beendet wird, sobald eine der Filterbedingungen erfüllt ist.

➤ Wählen Sie das gewünschte Interface, z. B. ***en1***, und bestätigen Sie mit der **Eingabetaste**.

Folgendes Menü öffnet sich bei Ethernet-Interfaces:

```
X4x00 Setup Tool                              BinTec Access Networks GmbH
[QoS][INTERFACES][EDIT]: Configure QoS Policies                  MyRouter

        Interface                     en1
        IP QoS Classification via     RI 1 FI 1 (test1)


                          SAVE                        CANCEL

Use <Space> to select
```

Das Feld des Menüs ***QoS*** ➧ ***Interfaces and Policies*** ➧ **EDIT** für Ethernet-Interfaces:

Feld	Bedeutung
IP QoS Classification via	Legt den Interface-spezifischen "Einsprung" in eine Regelkette fest. Zu klassifizierende Pakete werden dann beginnend mit dieser ersten Regel und dem zugehörigen IP-Filter untersucht.

Tabelle 7-54: ***QoS*** ➧ ***Interfaces and Policies*** ➧ **EDIT**

IP-Paket-Klassifizierung aktivieren

Gehen Sie folgendermaßen vor, um die Klassifizierung für das gewünschte Interface zu aktivieren:

- Gehen Sie zu ***QoS*** ➧ ***Interfaces and Policies***.
- Wählen Sie das gewünschte Interface und bestätigen Sie mit der **Eingabetaste**.

Es kann immer nur eine Regelkette pro Interface erstellt werden. Sollen also mehrere IP-Filter auf einem Interface angewandt werden, so müssen diese über eine Regelkette miteinander verbunden werden. Besondere Sorgfalt ist erforderlich, falls es Überschneidungen zwischen mehreren Filtern gibt (Schnitt- bzw. Untermengen). Hier muß beachtet werden, daß die Abarbeitung einer Regelkette für jedes IP-Paket beendet wird, sobald eine der Filterbedingungen erfüllt ist.

- Wählen Sie die gewünschte erste anzuwendende Regel bei **IP QoS Classification via** aus.
- Bestätigen Sie mit **SAVE** und **EXIT**.

  Sie befinden sich wieder im Menü ***QoS***. Die Eintragungen sind temporär gespeichert und aktiviert.
- Fahren Sie für WAN-Interfaces gegebenenfalls fort mit Kapitel 7.4.4, Seite 271.

7.4.4 QoS-Bandbreitenmanagement (Policies) festlegen

QoS auf WAN-Interface

Ist QoS auf einem WAN-Interface aktiviert, so sind zusätzlich Einstellungen im Untermenü ***QoS*** ➧ ***Interfaces and Policies*** vorzunehmen. Diese Einstellungen betreffen die Behandlung ("Policy") mit den zuvor klassifizierten IP-Paketen, also z. B. die Queueing- und Discard-Strategien für diese Paketklassen.

Sendeseitig wird mit mindestens drei Queues gearbeitet: eine Queue für die "high-priority" Daten, 1 bis 255 Queues für die mit *normal* priorisierten Daten und (Default) Queue für alle nicht klassifizierten Daten. Die Zahl der Queues normaler Priorität (von Typ "class-based") entspricht der Anzahl der "Policy"-Einträge für diese Klasse (Menü ***QoS*** ➧ ***Interfaces and Policies*** ➧ **EDIT** ➧ ***Class-Based QoS Policies*** ➧ **ADD**), so daß für bis zu 255 Klassen von Paketen (siehe Kapitel 7.4.2, Seite 263) eine eigene Queue (mit entsprechender "Policy") eingerichtet werden kann. Alle entweder nicht klassifizierten oder keiner Klasse zugeordneten Pakete, für die es keine definierte "Policy" gibt, werden über eine Default-Queue abgearbeitet. Für die Default-Queue kann ebenfalls eine eigene "Policy" definiert werden und diese somit in das Queueing- und Scheduling-Verfahren einbezogen werden. Dagegen kann für die "high-priority" Queue sinnvollerweise lediglich eine Bandbreitenbeschränkung definiert werden.

Algorithmen

Derzeit sind drei Scheduling-Algorithmen implementiert (Nur für die Bedienung der "normal"- und "default"-Queues relevant):

- "Priority Queueing" (PQ): Über die Priorität einer Queue wird die Reihenfolge der Bedienung festgelegt. Eine Queue wird erst bedient, wenn alle anderen Queues höherer Priorität leer sind.

- "Weighted Round-Robin Scheduling" (WRR): Über die zu definierende Gewichtung wird die Häufigkeit der Bedienung der Queues in Relation zueinander festgelegt.
- "Weighted Fair Queueing" (WFQ): Unterschiedliche Datenströme (Traffic Flows) werden dabei möglichst fair bedient, so daß (innerhalb einer Queue bzw. Klasse) nicht eine Verbindung auf Kosten der anderen überproportional Bandbreite konsumieren kann.

Nur frei verfügbare Bandbreite wird über diese Algorithmen verteilt. Queues, deren reservierte Bandbreite noch nicht voll ausgenutzt worden ist, werden vorrangig bedient. Unabhängig vom gewählten Queueing- und Scheduling-Verfahren wird die "high-priority"-Queue immer vorrangig bedient.

Traffic Shaping "Traffic Shaping" spezifiziert eine maximale Bitübertragungsrate für ein Interface. Diese Limitierung schließt alle zu sendenden Daten mit ein (sowohl *high-priority* und *normal* als auch System-Messages wie "Keepalive", "RIP", usw.). "Traffic Shaping" wird insbesondere für die Bandbreitenlimitierung von virtuellen (WAN-)Interfaces bzw. -Verbindungen benötigt, die über ein Interface mit einer höheren Bandbreite aufgebaut werden, z. B. "PPP over PPTP" oder auch PPPoE, also WAN-Verbindungen, welche über Ethernet realisiert werden.

Policy Für jede Klasse kann eine "Policy" definiert und somit festgelegt werden, in welcher Queue ein zu sendendes Paket im Rahmen des konfigurierten Scheduling-Verfahrens bearbeitet wird. Der Typ der Queue bzw. die Art der möglichen Konfiguration wird von der Paketklasse bestimmt, für welche die "Policy" gelten soll. Es ist zu unterscheiden – wie auch schon zuvor bei der Klassifizierung – zwischen der "high-priority" und den bis zu 255 "normal" Klassen, für die entsprechende Queues bzw. "Policies" definiert werden können. Hinzu kommt noch eine Default-Queue/Klasse für alle nicht zuvor klassifizierten Pakete. Auch für diese Klasse kann eine "Policy" definiert werden.

Es ist möglich, jeder Queue und somit jeder Paketklasse einen bestimmten Anteil an der Gesamtbandbreite des Interfaces zuzuweisen bzw. zu garantieren.

Pakete vom Typ "high-priority" haben immer Vorrang vor den anderen Daten. Somit wird bei inkonsistenter Konfiguration (Summe der einzelnen, reservierten Bandbreitenanteile ist größer als die Gesamtbandbreite) zugunsten der "high-priority"-Daten u. U. auch reservierte Bandbreite der "normal" Queues herangezogen.

Congestion Avoidance

TCP-Verbindungen reagieren auf Paketverluste üblicherweise mit einer (temporären) Verringerung ihrer Übertragungsrate. Verwirft man zu sendende Pakete mit einer zum mittleren Füllstand der Queue proportionalen Wahrscheinlichkeit, so kann man dafür sorgen, daß die Queue im Mittel kleiner bleibt und die maximale Queue-Größe, ab der Pakete verworfen werden, seltener erreicht wird. Außerdem werden ein im Mittel kleinerer Transit-Delay und signifikant kleinere Verlustraten erreicht, falls Bursts die Größe der Queue doch mal soweit ansteigen lassen sollten, daß die sogenannten Dropping-Algorithmen eingreifen. RED (Random Early Detection) – sofern konfiguriert – ist aktiv bei Queue-Größen zwischen "Lower Queue Threshold"- und "Upper Queue Threshold"-Schwellwerten.

Dieser Algorithmus greift nur, sofern überwiegend Daten auf TCP-Basis (z. B. per FTP) übertragen werden und die jeweiligen TCP-Implementationen standardkonform arbeiten, sich also kooperativ gegenüber dieser speziellen Art der Signalisierung verhalten. Andere Datenströme z. B. auf UDP-Basis (wie RTP) lassen sich hiermit dagegen nicht beeinflussen.

Schwellwerte

Die Bedeutung der Schwellwerte "Lower Queue Threshold" und "Upper Queue Threshold" für die einzelne Queue läßt sich am einfachsten mit der nachfolgenden Skizze darstellen:

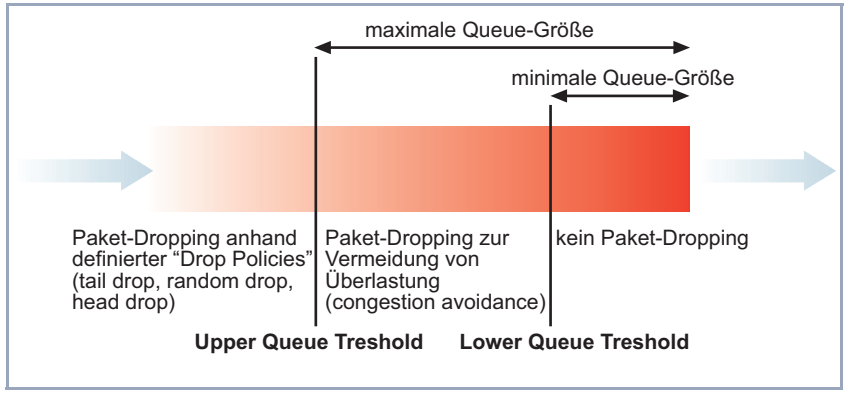


Bild 7-5: Bedeutung der Schwellwerte einer Queue

Bei einer Queue-Größe, die unterhalb des Schwellwertes "Lower Queue Threshold" liegt, werden weder "Dropping"- noch "Congestion Avoidance"-Algorithmen angewandt.

Bei einer Queue-Größe, die maximal den Schwellwert "Upper Queue Threshold" annimmt, wird je nach definiertem Dropping-Algorithmus versucht, die Queue nicht weiter anwachsen zu lassen.

Überschreitet die Queue den Schwellwert "Upper Queue Threshold", werden Pakete nach der definierten "Drop-Policy" verworfen.

Multilink PPP (MLPPP)

Hierbei handelt es sich um einen speziellen PPP-Modus für vergleichsweise schmalbandige WAN-Verbindungen wie z. B. ISDN, X.21 (64 kBit). Dieser Modus ermöglicht die Übertragung von als "high-priority" klassifizierten Daten mit einem Minimum an Verzögerung (Transit-Delay) verglichen mit einer normalen PPP-Verbindung. Dies wird dadurch erreicht, daß die als "normal" klassifizierten Pakete ab einer bestimmten (zu konfigurierenden) Größe fragmentiert werden, um bei Bedarf sofort ein "high-priority", nicht fragmentiertes Paket zwischen diese Fragmente schieben zu können.

Konfiguration

Haben Sie in Kapitel 7.4.3, Seite 269 ein WAN-Interface festgelegt, auf welchem die zuvor festgelegte Klassifizierung erfolgen soll, dann öffnet sich folgendes Menü:

```
X4x00 Setup Tool                          BinTec Access Networks GmbH
[QoS][INTERFACES][EDIT]: Configure QoS Policies               MyRouter

        Interface                     dialup1

        IP QoS Classification via     RI 4 FI 4 (test2)

        QoS Scheduling and Shaping
        Class-Based QoS Policies

        MLPP Interleave Mode          yes
        MLPPP Fragment Size           250

                        SAVE                        CANCEL

Use <Space> to select
```

Das Untermenü ***QoS*** ➧ ***INTERFACES AND POLICIES*** ➧ **EDIT** ➧ ***QoS SCHEDULING AND SHAPING*** hat folgende Auswahlmöglichkeiten:

Feld	Bedeutung
Queueing and Scheduling Algorithm	Aktiviert bzw. deaktiviert QoS auf dem WAN-Interface. Die zuvor klassifizierten Daten werden also auf einzelne Queues aufgeteilt, die dann mit unterschiedlichen Algorithmen bedient werden können. Mögliche Werte: ■ *disabled* Kein QoS auf diesem Interface, zuvor klassifizierten Pakete werden wie bisher nach dem FIFO-Verfahren versendet. Der Eintrag wird aber nicht aus der Konfiguration gelöscht und kann bei Bedarf wieder aktiviert werden. ■ *delete* Der Eintrag wird gelöscht. QoS wird auf dem Interface deaktiviert. ■ *prioritiy queueing (PQ)* Frei verfügbare Bandbreite wird nach einer (definierten) Priorisierung verteilt (siehe **Priority**, Tabelle 7-56, Seite 280). Eine Queue wird erst bedient, wenn alle anderen Queues höherer Priorität leer sind (nur für "normal" und "default" Klasse relevant). ■ *weighted round-robin scheduling (WRR)* (nur für "normal"- und "default"-Queue relevant) Frei verfügbare Bandbreite wird nach einer (definierten) Gewichtung verteilt (siehe **Weight**, Tabelle 7-56, Seite 280).

Feld	Bedeutung
noch **Queueing and Scheduling Algorithm**	■ *weighted fair queueing (WFQ)* (nur für "normal"- und "default"-Queue relevant) Frei verfügbare Bandbreite wird möglichst "fair" unter den (selbsttätig erkannten) Datenverbindungen (Traffic-Flows) aufgeteilt.
Specify Traffic Shaping	Aktiviert bzw. deaktiviert eine Bandbreitenlimitierung ("Shaping" in Bits pro Sekunde) auf dem Interface. Nur einstellbar, wenn für **Queueing and Scheduling Algorithm** nicht *delete* oder *disabled* gewählt wurde. Diese Limitierung betrifft auch "high-priority" Daten. Mögliche Werte: ■ *yes* ("Shaping" aktiviert) ■ *no* ("Shaping" deaktiviert)
Maximum Transmit Rate (Bits per Second)	Nur einstellbar, wenn **Specify Traffic Shaping** auf *yes* gesetzt ist. Hier wird die maximale Bandbreite des Interfaces (in Senderichtung) angegeben. Mögliche Werte: *0* bis *2048000*.

Tabelle 7-55: ***QoS*** ➧ ***Interfaces and Policies*** ➧ **EDIT** ➧ ***QoS Scheduling and Shaping***

Im Untermenü ***QoS*** ➧ ***Interfaces and Policies*** ➧ **EDIT** ➧ ***Class-Based QoS Policies*** ➧ **ADD** sind folgende Auswahlmöglichkeiten relevant:

Feld	Bedeutung
Class	Definiert, für welche Paketklasse diese "Policy" gelten soll. Mögliche Werte: ■ *default*: "Policy" für Daten, die nicht explizit einer Queue zugeordnet wurden (Nur ein Eintrag sinnvoll). ■ *class-based*: "Policy" für "normal"-Klassen. ■ *high priority*: "Policy" für "high-priority"-Klasse (Nur ein Eintrag sinnvoll).
Class ID	Nur einstellbar für den Wert *class-based* im Feld **Class**. Durch die **Class ID** erfolgt die Zuordnung der "normal"-Klasse zur Queue bzw. "Policy". Möglich sind alle IDs, die für die Klassifizierung definiert wurden.
Transmit Rate (Bits per Second)	Definiert die für diese Klasse zu reservierende Bandbreite in Bits pro Sekunden. Dieser Anteil an der Bandbreite des Interfaces darf für andere Daten nur dann genutzt werden, wenn keine Pakete dieser Klasse zu versenden sind. Mögliche Werte: *0* bis *2048000*.
Bound Transmit Rate (Shaping)	Definiert, ob der für diese Klasse reservierte Bandbreitenanteil überschritten werden darf (im längerfristigen Mittel) oder nicht. Nur einstellbar, wenn der Wert für **Transmit Rate (Bits per Second)** größer als Null ist. Mögliche Werte: ■ *yes* (bounded): Reservierte Bandbreite ist zugleich die Obergrenze. ■ *no* (not bounded): Anderweitig nicht benötigte Bandbreite darf auch von dieser Klasse verbraucht werden.

Feld	Bedeutung
Transmit Rate Burst	Definiert die maximale Anzahl von Bytes, die noch übertragen werden dürfen, wenn der für diese Queue ermittelte Durchsatz dem reservierten Wert entspricht. Nur einstellbar, wenn der Wert für **Transmit Rate (Bits per Second)** größer als Null ist. Mögliche Werte: *0* bis *64000*.
Weight	Relative Gewichtung dieser Klasse. Nur relevant für den Wert *weighted round-robin scheduling (WRR)* bei **Queueing and Scheduling Algorithm** und für die Werte *default* und *class-based* bei **Class**. Mögliche Werte: *1* bis *255*.
Priority	Relative Priorität innerhalb der "normal"-Klasse/Queue. Nur relevant für den Wert *prioritiy queueing (PQ)* bei **Queueing and Scheduling Algorithm** und für die Werte *default* und *class-based* bei **Class**. Mögliche Werte: *0* bis *255*. Je kleiner der Wert, desto höher die Priorität.
Shaping Algorithm	Keine Auswahlmöglichkeit. Bisher nur Token-Bucket-Verfahren bei der Zuweisung/Limitierung der Bandbreite für eine Queue.

Feld	Bedeutung
Congestion Avoidance Algorithm	Definiert das Verfahren, nach dem bei Erreichen des "Lower Queue Threshold" für diese Queue neu hinzukommende, zu versendende Pakete behandelt werden; d. h. ob diese bedingungslos "eingequeuet" oder ggf. verworfen werden. Mögliche Werte: ■ *none*: Pakete werden auf jeden Fall in die Queue aufgenommen. ■ *weighted-random (RED)*: Pakete werden mit einer errechneten Wahrscheinlichkeit proportional zur längerfristig ermittelten mittleren Queue-Größe verworfen. Dieses Verfahren sorgt bei TCP-basierten Datenverkehr für eine längerfristig kleinere Queue-Größe, so daß auch Traffic-Bursts zumeist ohne größere Paketverluste übertragen werden können.
Dropping Algorithm	Spezifiziert, nach welchem Verfahren – nach dem bei Erreichen des "Upper Queue Threshold" (entspricht der maximalen Größe dieser Queue) – für diese Klasse/Queue neu hinzukommende, zu versendende Pakete verworfen werden. Mögliche Werte: ■ *tail-drop*: Das neu hinzugekommene Paket wird verworfen. ■ *head-drop*: Das älteste Paket in der Queue wird verworfen. ■ *random-drop*: Ein zufällig ausgewähltes Paket aus der Queue wird verworfen.

Feld	Bedeutung
Lower Queue Treshold	Definiert die minimale Queue-Größe, unterhalb welcher weder "Dropping"- noch "Congestion Avoidance"-Algorithmen angewandt werden. Mögliche Werte: *0* bis *256000*.
Upper Queue Treshold	Definiert die maximale Queue-Größe. Bei Erreichen dieses Schwellwertes wird je nach definiertem **Dropping Algorithm** versucht, die Queue nicht weiter anwachsen zu lassen. Mögliche Werte: *0* bis *256000*.

Tabelle 7-56: ***QoS*** ➧ ***Interfaces and Policies*** ➧ **EDIT** ➧ ***Class-Based QoS Policies*** ➧ **ADD**

Die Felder des Menüs ***QoS*** ➧ ***Interfaces and Policies*** ➧ **EDIT** bei Auswahl eines WAN-Interfaces:

Feld	Bedeutung
MLPPP Interleave Mode	Aktiviert/Deaktiviert den MLPPP-Interleave-Modus. Mögliche Werte: ■ *yes*: aktiviert den Multilink-PPP-Interleave-Modus für den bevorzugten Dienst der "high-priority"-Pakete auf langsamen PPP-Verbindungen. ■ *no*: deaktiviert den Multilink-PPP-Interleave-Modus.
MLPPP Fragment Size	Definiert die maximale Größe der Fragmente, in welche die "normal"-priorisierten Pakete aufgeteilt werden. Je kleiner der gewählte Wert, desto geringer die Latenzzeit für ein zu übertragendes "high-priority"-Paket. Nur einstellbar, wenn **MLPPP Interleave Mode** auf *yes* gesetzt ist. Mögliche Werte: *30* bis *1500*.

Tabelle 7-57: ***QoS*** ➧ ***Interfaces and Policies*** ➧ **EDIT**

Policies festlegen

Gehen Sie folgendermaßen vor, um ein entsprechendes QoS-Bandbreitenmanagement auf WAN-Verbindungen zu konfigurieren:

- Gehen Sie zu ***QoS*** ➧ ***Interfaces and Policies***.
- Wählen Sie das WAN-Interface aus, auf welchem das QoS-Bandbreitenmanagement aktiviert werden soll und bestätigen Sie mit der **Eingabetaste**.

  Sie befinden sich im Menü ***QoS*** ➧ ***Interfaces and Policies*** ➧ **EDIT**.
- Aktivieren Sie gegebenenfalls die Klassifikation **IP QoS Classification via** aus, wie in Kapitel 7.4.3, Seite 269 beschrieben.
- Gehen Sie zu ***QoS*** ➧ ***Interfaces and Policies*** ➧ **EDIT** ➧ ***QoS Scheduling and Shaping***.
- Wählen Sie den gewünschten **Queueing and Scheduling Algorithm** aus.

Traffic Shaping

- Wählen Sie *yes* für **Specify Traffic Shaping** aus und geben Sie **Maximum Transmit Rate (Bits per Second)** die gewünschte Bandbreite an, sofern Sie eine Bandbreitenlimitierung ("Traffic Shaping") für das WAN-Interface definieren möchten.
- Bestätigen Sie mit **OK**.

  Sie befinden sich wieder im Menü ***QoS*** ➧ ***Interfaces and Policies*** ➧ **EDIT**.

Policies für definierte Klassen konfigurieren

- Gehen Sie zu ***QoS*** ➧ ***Interfaces and Policies*** ➧ **EDIT** ➧ ***Class-Based QoS Policies***.
- Legen Sie mit **ADD** eine neue "Policy" an oder wählen Sie eine vorhandene "Policy" aus.
- Wählen Sie unter **Class** den Typ Klasse aus, für welchen diese "Policy" gelten soll.
- Wählen Sie gegebenenfalls eine **Class ID** aus.
  Diese haben Sie bei der Konfiguration der IP-Klassifikation definiert.
- Geben Sie den gewünschten Wert für **Transmit Rate (Bits per Second)** ein, sofern Sie eine Bandbreitenreservierung für diese Klasse vornehmen möchten.
- Definieren Sie mit **Bound Transmit Rate (Shaping)**, ob diese Bandbreite begrenzt ist (*yes*) oder nicht (*no*).

- Geben Sie den gewünschten Wert für **Transmit Rate Burst** ein, falls Sie **Bound Transmit Rate (Shaping)** auf *yes* gesetzt haben, also die Bandbreite begrenzt ist.
  Somit definieren Sie eine zulässige kurzzeitige Überschreitung (Burst) von **Transmit Rate (Bits per Second)**.
- Geben Sie die gewünschte relative Gewichtung für **Weight** ein, falls Sie für **Queueing and Scheduling Algorithm** *weighted round-robin scheduling (WRR)* gewählt haben.
- Geben Sie die gewünschte Priorität für diese Klasse bzw. der zugeordneten Queue bei **Priority** ein, falls Sie für **Queueing and Scheduling Algorithm** *prioritiy queueing (PQ)* gewählt haben.
- Wählen Sie gegebenenfalls *weighted-random (RED)* für **Congestion Avoidance Algorithm** aus, falls die zu übertragenden Daten vorwiegend über TCP-Verbindungen laufen.
- Wählen Sie den gewünschten **Dropping Algorithm** aus.
- Geben Sie den gewünschten Wert für **Lower Queue Treshold** ein (relevant für **Dropping Algorithm** bzw. *weighted-random (RED)*).
- Geben Sie den gewünschten Wert für **Upper Queue Treshold** ein (relevant für **Dropping Algorithm** bzw. *weighted-random (RED)*).
- Bestätigen Sie mit **OK**.
  Sie befinden sich im Menü ***QoS*** ➧ ***Interfaces and Policies*** ➧ **EDIT** ➧ ***Class-Based QoS Policies*** und sehen die Liste der bereits definierten "Policies".
- Wiederholen Sie die Eintragungen, bis Sie alle benötigten "Policies" konfiguriert haben.
- Verlassen Sie das Menü mit **EXIT**.
  Sie befinden sich wieder im Menü ***QoS*** ➧ ***Interfaces and Policies*** ➧ **EDIT**.

MLPPP Interleave Mode

- Aktivieren Sie gegebenenfalls für vergleichsweise langsame WAN-Verbindungen **MLPPP Interleave Mode** (*yes*).
  Dadurch kann die Latenzzeit für "high-priority" Pakete entscheidend verringert werden.

- Geben Sie für **MLPPP Fragment Size** die gewünschte maximale Fragmentgröße für ein Paket normaler Priorität ein, falls Sie **MLPPP Interleave Mode** auf *yes* gesetzt haben.
  Dieser Wert wird bestimmt durch die Bandbreite der Verbindung und der gewünschten Latenzzeit.
- Bestätigen Sie mit **SAVE**.

Menü verlassen

- Verlassen Sie das Menü ***QoS*** ➧ ***Interfaces and Policies*** mit **EXIT**.
  Sie befinden sich wieder im Menü ***QoS***.
- Verlassen Sie das Menü mit **EXIT**.
  Sie befinden sich wieder im Hauptmenü. Die Eintragungen sind temporär gespeichert und aktiviert.

7.5 Bridging

X4100/200/300 unterstützt die Funktion Bridging. Die Beschreibung der Konfiguration von **X4100/200/300** als Bridge finden Sie in der **Software Reference**.

7.6 Funktionen mit Zusatzlizenz

In diesem Kapitel wird kurz dargestellt, welche Funktionen Sie auf **X4100/200/300** mit einer Zusatzlizenz freischalten können.

Die entsprechenden Zusatzlizenzen schalten Sie frei, indem Sie die erhaltenen Lizenzinformationen im Setup Tool Menü ***LICENSES*** hinzufügen (siehe Kapitel 6.1.1, Seite 102).

Für folgende Funktionen sind derzeit Zusatzlizenzen erhältlich:

- X.25
- Frame Relay
- OSPF
- Virtual Private Network (VPN, PPTP)
- TAF (Token Authentication Firewall)
- IPSec (inklusive IPSec System-Software)

Detaillierte Informationen und Konfigurationshinweise (mit Beispielen) finden Sie in der **Software Reference** bzw. für IPSec in Ihrem **IPSec Reference Manual**.

8 Konfiguration der Erweiterungs- und Ressourcenkarten mit dem Setup Tool

In diesem Kapitel erfahren Sie, welche Konfigurationsschritte Sie vornehmen können, wenn Sie Ihr **X4100/200/300**-Grundgerät mit einer Erweiterungskarte und gegebenfalls mit Ressourcenkarten ausgestattet haben. Eingebaute Erweiterungs- bzw. Ressourcenkarten werden von **X4100/200/300** beim Starten automatisch erkannt.

Für die Installation der Erweiterungs- und Ressourcenkarten beachten Sie bitte die mit den Karten mitgelieferte Einbauanleitung bzw. Kapitel 3.3, Seite 39.

Tragen Sie gegebenenfalls erforderliche Lizenz(en) im Setup Tool ein (siehe Kapitel 6.1.1, Seite 102), bevor Sie mit der Konfiguration beginnen.

Dieses Kapitel ist folgendermaßen aufgebaut:

Achtung!

Der Einbau der PRI/G.703-Erweiterungskarte bzw. der Einbau von Ressourcenkarten in eine Erweiterungskarte führt zu verstärkter Wärmeentwicklung. Um die Schädigung von Bauteilen zu vermeiden, ist der Einsatz einer Lüfterkassette zwingend erforderlich!

➤ Setzen Sie bei Verwendung der PRI/G.703-Erweiterungskarte oder einer Erweiterungskarte mit Ressourcenkarte(n) im **X4100/200/300**-Einbaugerät die Lüfterkassette ein.

Sie können die Lüfterkassette von Ihrem Lieferanten käuflich erwerben.

- WAN-Schnittstellenkarte für ISDN-BRI (Basic Rate Interface) (Kapitel 8.1, Seite 289)
- WAN-Schnittstellenkarte für ISDN-PRI (Primary Rate Interface) und/oder G.703 (Kapitel 8.2, Seite 292)
- LAN-Schnittstellenkarte für 10/100 MBit/s (Kapitel 8.3, Seite 298)

- Ressourcenkarten mit Digitalmodems (Kapitel 8.4, Seite 300)
- Ressourcenkarte zur Verschlüsselung und Kompression (Kapitel 8.5, Seite 310)

8.1 WAN-Schnittstellenkarte für ISDN-BRI

Durch Installation einer Basic-Rate-Interface-Erweiterungskarte können Sie **X4100/200/300** mit bis zu drei zusätzlichen ISDN-BRI-Schnittstellen ausstatten. Diese Schnittstellen können Sie sowohl für Wähl- als auch für Festverbindungen über ISDN nutzen.

Die BRI-Erweiterungskarte können Sie optional mit einer Ressourcenkarte mit Digitalmodems (siehe Kapitel 8.4, Seite 300) und/oder mit einer Ressourcenkarte zur Verschlüsselung und Kompression (siehe Kapitel 8.5, Seite 310) ausstatten.

Setup Tool mit zusätzlichen Schnittstellen

Im Setup-Tool-Hauptmenü werden die zusätzlichen Schnittstellen unter **Module** folgendermaßen angezeigt:

```
X4x00 Setup Tool                              BinTec Access Networks GmbH
                                                                MyRouter

Licenses                  System

LAN:          CM-100BT,Fast Ethernet        Module:  X4E-3BRI,ISDN S0

WAN:          CM-1BRI,ISDN S0

Serial-WAN:   CM-SERIAL, Serial             Resources:

WAN Partner
IP      PPP      ISDN     CAPI     QoS

Configuration Management
Monitoring and Debugging
Exit
```

Die Konfiguration der Schnittstelle(n) erfolgt in den Menüs

- ***X4E-3BRI, ISDN S0*** ➧ ***UNIT 0*** für den ersten zusätzlichen ISDN-BRI-Port
- ***X4E-3BRI, ISDN S0*** ➧ ***UNIT 1*** für den zweiten zusätzlichen ISDN-BRI-Port
- ***X4E-3BRI, ISDN S0*** ➧ ***UNIT 2*** für den dritten zusätzlichen ISDN-BRI-Port

Die Anzahl der mit der Erweiterungskarte verfügbaren ISDN-BRI-Ports kann variieren, abhängig davon, wie viele Schnittstellen per Lizenz freigeschaltet werden. Die benötigten Lizenzen erhalten Sie gegebenenfalls von Ihrem Händler.

Konfiguration

Gehen Sie folgendermaßen vor, um die ISDN-BRI-Schnittstelle(n) der Erweiterungskarte zu konfigurieren:

- Gehen Sie zu ***X4E-3BRI, ISDN S0*** ➧ ***UNIT 0*** für die erste Schnittstelle. Dieses Menü bietet die gleichen Möglichkeiten wie ***CM-1BRI, ISDN S0*** für die ISDN-BRI-Schnittstelle des Grundgeräts.
- Konfigurieren Sie die Schnittstellen, wie in Kapitel 6.2.1, Seite 121 beschrieben.

Incoming Call Answering

Wenn über die ISDN-BRI-Schnittstelle Wählverbindungen aufgebaut werden sollen, teilen Sie **X4100/200/300** als nächstes die eigenen Rufnummern für diese Schnittstelle mit:

Bei einer Festverbindung sind diese Einstellungen nicht möglich.

- Gehen Sie zu ***X4E-3BRI, ISDN S0*** ➧ ***UNIT 0*** ➧ ***INCOMING CALL ANSWERING***.

  In diesem Menü sind die bisher vorgenommenen Zuteilungen der Dienste zu den Rufnummern aufgelistet, es bietet die gleichen Möglichkeiten wie ***CM-1BRI, ISDN S0*** ➧ ***INCOMING CALL ANSWERING*** für die Verteilung der eingehenden Rufe über die ISDN-BRI-Schnittstelle des Grundgeräts. Für detaillierte Erklärungen beachten Sie bitte "Incoming Call Answering", Seite 125.
- 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.
- Wählen Sie **Item** aus, z. B. ***PPP (routing)***.
- Geben Sie **Number** ein, z. B. ***12330***.
- 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 ***X4E-3BRI, ISDN S0*** ➧ ***UNIT 0*** ➧ ***INCOMING CALL ANSWERING***. Die Eintragungen sind temporär gespeichert und aktiviert und werden in der Liste angezeigt.

  Sie haben damit einer Ihrer Rufnummern (*123 30*) einen möglichen Dienst (*PPP (routing)*) zugeordnet. Wenn also ein Datenruf an die Called Party's Number *123 30* eingeht, wird er an den Dienst PPP (routing) weitergeleitet. Veranlaßt der Dienst PPP (routing) einen abgehenden Datenruf, dann wird als Calling Party's Number die *12330* zugeordnet.
- Wiederholen Sie diese Schritte, bis Sie allen Rufnummern die Dienste zugeordnet haben, die unter diesen Rufnummern erreichbar sein sollen.

  Damit haben Sie Incoming Call Answering für diese ISDN-BRI-Schnittstelle konfiguriert. **X4100/200/300** verteilt die eingehenden Rufe an die internen Dienste bzw. verwendet bei abgehenden Rufen die jeweils zugewiesene **Number**.
- Verlassen Sie ***X4E-3BRI, ISDN S0*** ➧ ***UNIT 0*** ➧ ***INCOMING CALL ANSWERING*** mit **EXIT**.
- Bestätigen Sie mit **SAVE**.
- Gehen Sie gegebenenfalls zu ***X4E-3BRI, ISDN S0*** ➧ ***UNIT 1*** für die Konfiguration der zweiten Schnittstelle.
- Gehen Sie gegebenenfalls zu ***X4E-3BRI, ISDN S0*** ➧ ***UNIT 2*** für die Konfiguration der dritten Schnittstelle.

WAN-Partner

Um mit **X4100/200/300** Verbindungen zu Netzwerken oder Hosts außerhalb Ihres LANs herstellen zu können, müssen Sie die gewünschten Verbindungspartner als WAN-Partner auf **X4100/200/300** einrichten. Dies gilt sowohl für Wählverbindungen als auch für Festverbindungen. Beachten Sie dazu Kapitel 6.3, Seite 147.

8.2 WAN-Schnittstellenkarte für ISDN-PRI und/oder G.703

Die Primary-Rate-Interface- bzw. G.703-Erweiterungskarte verfügt über zwei Ports mit jeweils zwei Buchsen (IN und OUT). Durch Installation der Erweiterungskarte können Sie **X4100/200/300** wahlweise mit folgenden Schnittstellen ausstatten:

- Eine ISDN-PRI- und/oder eine G.703-Schnittstelle
- Zwei ISDN-PRI-Schnittstellen
- Zwei G.703-Schnittstellen

Die erforderlichen Lizenzen zum Freischalten der gewünschten Schnittstellen erhalten Sie von Ihrem Händler.

PRI Eine ISDN-PRI-Schnittstelle von **X4100/200/300** können Sie an einen Primärmultiplexanschluß anschließen. Verbinden Sie dazu den Network-Termination-Adapter Ihrer Telefongesellschaft mit der IN-Buchse eines per Lizenz freigeschalteten Ports. In Deutschland stehen Ihnen damit 30 B-Kanäle und ein D-Kanal zur Verfügung, die Sie sowohl für Wähl- als auch für Festverbindungen über ISDN nutzen können.

G.703 Mit einer G.703-Schnittstelle von **X4100/200/300** können Sie eine G.703-Festverbindung zu einem Verbindungspartner installieren. Verbinden Sie dazu ebenfalls den NT-Adapter Ihrer Telefongesellschaft mit der IN-Buchse eines per Lizenz freigeschalteten Ports. Eine G.703-Festverbindung ist eine unstrukturierte Hochgeschwindigkeitsleitung mit bis zu zwei MBit/s für die Übertragung von Daten mit HDLC-Framing. Der Verbindungszustand wird nicht auf Schicht 1 kontrolliert, dies muß gegebenenfalls von höheren Protokollschichten wie dem PPP übernommen werden.

Eine PRI-Schnittstelle können Sie sowohl als PRI- als auch als G.703-Schnittstelle nutzen.

Eine G.703-Schnittstelle könne Sie nur als G.703-Schnittstelle nutzen.

Die PRI- bzw. G.703-Erweiterungskarte ist im Auslieferungszustand mit Hardware-Unterstützung für Verschlüsselung und Kompression ausgestattet

(Kapitel 8.5, Seite 310) und kann optional mit bis zu zwei Ressourcenkarten mit Digitalmodems (Kapitel 8.4, Seite 300) aufgerüstet werden.

Setup Tool mit zusätzlichen Schnittstellen

Im Setup-Tool-Hauptmenü werden die zusätzlichen Schnittstellen unter **Module** folgendermaßen angezeigt:

```
X4x00 Setup Tool                              BinTec Access Networks GmbH
                                                                MyRouter

Licenses                  System

LAN:          CM-100BT,Fast Ethernet       Module:  X4E-2PRI, ISDN S2M

WAN:          CM-1BRI,ISDN S0

Serial-WAN:   CM-SERIAL, Serial            Resources:

WAN Partner
IP       PPP      ISDN     CAPI     QoS

Configuration Management
Monitoring and Debugging
Exit
```

Die Konfiguration der ISDN-PRI/G.703-Schnittstelle(n) erfolgt in den Menüs:

- ***X4E-2PRI, ISDN S2M*** ➧ ***UNIT 0*** für den ersten ISDN-PRI/G.703-Port
- ***X4E-2PRI, ISDN S2M*** ➧ ***UNIT 1*** für den zweiten ISDN-PRI/G.703-Port

Die Anzahl der mit der Erweiterungskarte verfügbaren ISDN-PRI- bzw. G.703-Ports kann variieren, abhängig davon, wie viele und welche Schnittstellen per Lizenz freigeschaltet werden. Die benötigten Lizenzen erhalten Sie gegebenenfalls von Ihrem Händler.

Die Menüs enthalten 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.

Feld	Bedeutung
ISDN Switch Type	Definiert das ISDN-➤➤ **Protokoll**, das Ihnen Ihre Telefongesellschaft zur Verfügung stellt. Mögliche Werte: ■ *autodetect on bootup:* automatische D-Kanalerkennung (Standardeinstellung) ■ *Euro ISDN S2M user profile (TE)* ■ *Euro ISDN S2M network profile (NT)* ■ *leased line B1..B30* ■ *leased line, 1 Hyperchannel* ■ *leased line, chann. E1, 31 diff. endpoints*: Dieser Typ von Festverbindung wird in UK auch als "aggregated kilostream" bezeichnet. ■ *back to back* ■ *G.703*: Erforderlich, wenn Sie eine G.703-Festverbindung über die Schnittstelle einrichten wollen.
ISDN Line Framing	Mögliche Werte: ■ *standard (CRC4)* (Standardeinstellung) ■ *special (no CRC)* In den meisten Fällen wird für eine PRI-Schnittstelle die Standardeinstellung genutzt. In manchen Fällen in Schweden und Frankreich, wenn **X4100/200/300** an eine TK-Anlage angeschlossen ist, ist die Einstellung *special (no CRC)* erforderlich.

Feld	Bedeutung
Clock Mode	Definiert, welcher Verbindungspartner das Taktsignal zur Synchronisation zwischen Sender und Empfänger gibt. Wenn das Taktsignal nicht vom (TK)-Netz selbst erzeugt wird, muß einer der beiden Verbindungspartner dies tun. Mögliche Werte: ■ *extern* (Standardeinstellung): **X4100/200/300** empfängt das Taktsignal ■ *intern*: **X4100/200/300** gibt das Taktsignal

Tabelle 8-1: ***X4E-2PRI, ISDN S2M*** ➧ ***UNIT 0*** bzw. ***X4E-2PRI, ISDN S2M*** ➧ ***UNIT 1***

Konfiguration

Gehen Sie folgendermaßen vor, um die PRI-Schnittstelle für Wählverbindungen einzurichten:

➤ Gehen Sie zu ***X4E-2PRI, ISDN S2M*** ➧ ***UNIT 0*** für die erste ISDN-PRI-Schnittstelle.

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

Mit dieser Einstellung nutzt **X4100/200/300** 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 S2M user profile (TE)***.

Bei falsch eingestelltem ISDN-Protokoll kann kein ISDN-Verbindungsaufbau erfolgen und die Vermittlungsstelle des Providers schaltet evtl. die Leitung bei Nicht-Benutzen ab!

Achten Sie daher darauf, ob **X4100/200/300** das verwendete ISDN-Protokoll richtig erkennt und unter **Result of autoconfiguration** anzeigt. Falls dies nicht der Fall ist, tragen Sie es unter **ISDN Switch Type** manuell ein. Die automatische D-Kanal-Erkennung ist dann ausgeschaltet.

➤ Wählen Sie **ISDN Line Framing** aus, z. B. ***standard (CRC4)***.

➤ Wählen Sie **Clock Mode** aus, z. B. ***extern***.

Incoming Call Answering

Wenn über die ISDN-PRI/G.703-Schnittstelle Wählverbindungen aufgebaut werden sollen, teilen Sie **X4100/200/300** als nächstes die eigenen Rufnummern für diese Schnittstelle mit:

Bei einer Festverbindung sind diese Einstellungen nicht möglich.

- Gehen Sie zu ***X4E-2PRI, ISDN S2M*** ➧ ***UNIT 0*** ➧ ***INCOMING CALL ANSWERING***.

  In diesem Menü sind die bisher vorgenommenen Zuteilungen der Dienste zu den Rufnummern aufgelistet. Das Menü bietet die gleichen Möglichkeiten wie ***CM-1BRI, ISDN S0*** ➧ ***INCOMING CALL ANSWERING*** für die Verteilung der eingehenden Rufe über die ISDN-BRI-Schnittstelle des Grundgeräts. Für detaillierte Erklärungen beachten Sie bitte "Incoming Call Answering", Seite 125.

- 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.
- Wählen Sie **Item** aus, z. B. ***PPP (routing)***.
- Geben Sie **Number** ein, z. B. ***30***.
- 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 ***X4E-2PRI, ISDN S2M*** ➧ ***UNIT 0*** ➧ ***INCOMING CALL ANSWERING***. Die Eintragungen sind gespeichert und werden in der Liste angezeigt.

  Sie haben damit einer Ihrer Rufnummern (*30*) einen möglichen Dienst (*30*) zugeordnet. Wenn also ein Datenruf an die Called Party's Number 30 eingeht, wird er an den Dienst PPP (routing) weitergeleitet. Veranlaßt der Dienst PPP (routing) einen abgehenden Datenruf, dann wird als Calling Party's Number die *30* zugeordnet.

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

  Damit haben Sie Incoming Call Answering für diese ISDN-PRI-Schnittstelle konfiguriert, **X4100/200/300** verteilt die eingehenden Rufe an die internen Dienste bzw. verwendet bei abgehenden Rufen die jeweils zugewiesene **Number**.

- Verlassen Sie ***X4E-2PRI, ISDN S2M*** ➧ ***UNIT 0*** ➧ ***INCOMING CALL ANSWERING*** mit **EXIT**.

- Bestätigen Sie mit **SAVE**.

- Gehen Sie gegebenenfalls zu ***X4E-2PRI, ISDN S2M*** ➧ ***UNIT 1*** für die Konfiguration der zweiten ISDN-PRI/G.703-Schnittstelle.

WAN-Partner

Um mit **X4100/200/300** Verbindungen zu Netzwerken oder Hosts außerhalb Ihres LANs herstellen zu können, müssen Sie die gewünschten Verbindungspartner als WAN-Partner auf **X4100/200/300** einrichten. Dies gilt sowohl für Wählverbindungen als auch für Festverbindungen. Beachten Sie dazu Kapitel 6.3, Seite 147.

8.3 LAN-Schnittstellenkarte für 10/100 MBit/s

Durch Installation einer LAN-Erweiterungskarte können Sie **X4100/200/300** mit zwei zusätzlichen LAN-Schnittstellen ausstatten.

Die LAN-Erweiterungskarte können Sie optional mit einer Ressourcenkarte zur Verschlüsselung und Kompression (siehe Kapitel 8.5, Seite 310) ausstatten.

Setup Tool mit zusätzlichen Schnittstellen

Im Setup-Tool-Hauptmenü werden die zusätzlichen Schnittstellen unter **Module** folgendermaßen angezeigt:

```
X4x00 Setup Tool                              BinTec Access Networks GmbH
                                                                MyRouter

Licenses                  System

LAN:         CM-100BT,Fast Ethernet   Module:  X4E-100BT,FastEthernet


WAN:         CM-1BRI,ISDN S0

Serial-WAN:  CM-SERIAL, Serial        Resources:

WAN Partner
IP      PPP      ISDN     CAPI     QoS

Configuration Management
Monitoring and Debugging
Exit
```

Die Konfiguration der Schnittstellen erfolgt in den Menüs:

- ***X4E-100BT, FAST ETHERNET*** ➧ ***UNIT 0*** für die erste zusätzliche LAN-Schnittstelle
- ***X4E-100BT, FAST ETHERNET*** ➧ ***UNIT 1*** für die zweite zusätzliche LAN-Schnittstelle

Konfiguration

Gehen Sie folgendermaßen vor, um die LAN-Schnittstelle(n) der Erweiterungskarte zu konfigurieren:

Die Konfiguration der LAN-Erweiterungskarte für den Breitband-Internetzugang entspricht der Konfiguration der 10-Base-T-Ethernet-Schnittstelle der Grundgeräte **X4100** und **X4200** für den Breitband-Internetzugang und ist in Kapitel 6.2.3, Seite 138 beschrieben.

- Gehen Sie zu ***X4E-100BT, FAST ETHERNET*** ➧ ***UNIT 0*** für die erste Schnittstelle.
  Dieses Menü bietet die gleichen Möglichkeiten wie ***CM-100BT, FAST ETHERNET*** für die LAN-Schnittstelle des Grundgeräts. Für detaillierte Erklärungen beachten Sie bitte Kapitel 6.2.1, Seite 121.
- Geben Sie **local IP-Number** ein, z. B. ***192.168.1.250***.
- Geben Sie **local Netmask** ein, z. B. ***255.255.255.0***.
- Geben Sie gegebenenfalls **Second Local IP-Number** und **Second Local Netmask** ein.
- Wählen Sie **Encapsulation** aus, z. B. ***Ethernet II***.
- Wählen Sie **Mode** aus, z. B. ***Auto***.
- Bestätigen Sie mit **SAVE**.
  Sie befinden sich wieder im Hauptmenü, die Eintragungen sind temporär gespeichert und aktiviert.

Weiterführende Konfiguration

Informationen zu Bridging finden Sie in der **Software Reference**.

8.4 Ressourcenkarte mit Digitalmodems

ISDN-BRI- und ISDN-PRI/G.703-Erweiterungskarten (siehe Kapitel 8.1, Seite 289 bzw. Kapitel 8.2, Seite 292) können zusätzlich mit Ressourcenkarten mit Digitalmodems ausgestattet werden.

Ressourcenkarten mit Digitalmodems sind in unterschiedlichen Ausführungen erhältlich:

- XT-S: Ressourcenkarte mit 8 Digitalmodems
- XT-M: Ressourcenkarte mit 12 Digitalmodems
- XT-2M: Ressourcenkarte mit 24 Digitalmodems
- XT-L: Ressourcenkarte mit 30 Digitalmodems

Ausgerüstet mit Ressourcenkarte(n) mit Digitalmodems für analoge Verbindungen kann **X4100/200/300** als Remote-Access-Server für ISDN- und GSM-Verbindungen sowie für analoge Verbindungen (Dial-In und Dial-Out) genutzt werden.

Achtung!

Der Einbau der PRI/G.703-Erweiterungskarte bzw. der Einbau von Ressourcenkarten in eine Erweiterungskarte führt zu verstärkter Wärmeentwicklung. Um die Schädigung von Bauteilen zu vermeiden, ist der Einsatz einer Lüfterkassette zwingend erforderlich!

➤ Setzen Sie bei Verwendung der PRI/G.703-Erweiterungskarte oder einer Erweiterungskarte mit Ressourcenkarte(n) im **X4100/200/300**-Einbaugerät die Lüfterkassette ein.

Sie können die Lüfterkassette von Ihrem Lieferanten käuflich erwerben.

X4100/200/300 mit Digitalmodems

Ausgerüstet mit Digitalmodems kann **X4100/200/300** für Modemverbindungen genutzt werden, z. B. von Home-Office-Mitarbeitern mit analogen Modems oder von Außendienstmitarbeitern mit Laptop, Handy und Modem.

X4100/200/300 nutzt die Digitalmodems der Ressourcenkarte(n) als Modem-Pool und verwendet bei ein- und ausgehenden Modemverbindung immer dynamisch das nächste verfügbare Modem.

Hier eine grafische Darstellung einer Dial-In-Prozedur:

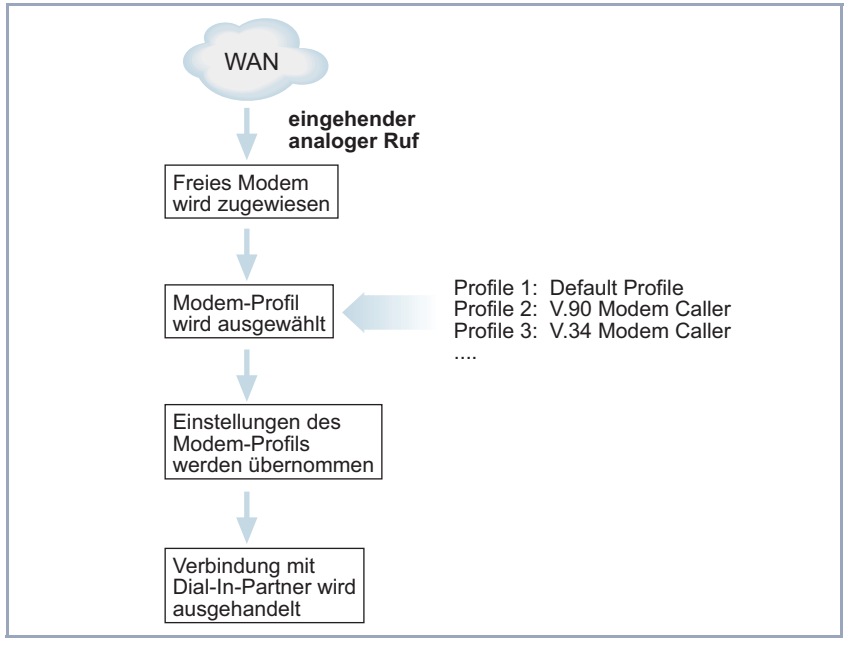


Bild 8-1: Dial-In auf **X4100/200/300** mit Digitalmodems

Modemprofile

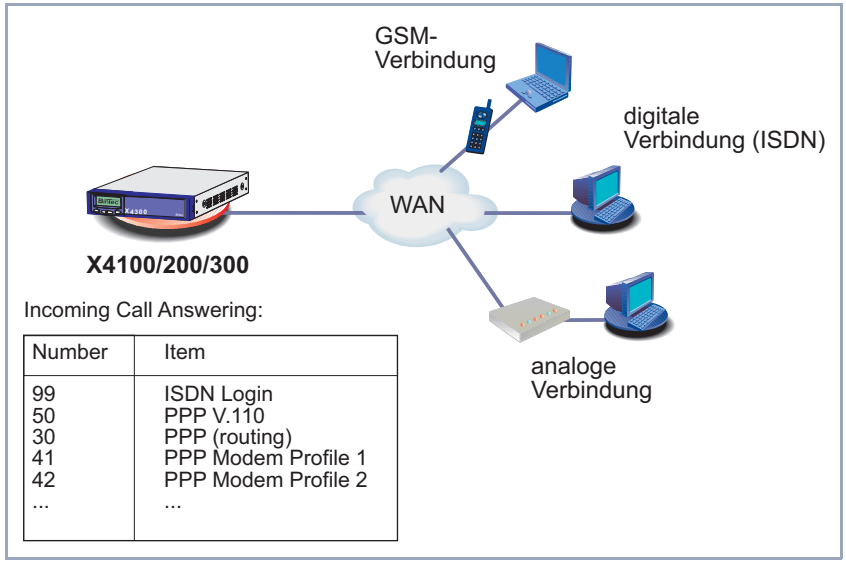
Die Modems (z. B. 30 Modems bei einer Ressourcenkarte XT-L) müssen nicht einzeln konfiguriert werden, da **X4100/200/300** ein flexibles Konzept von Modemprofilen verwendet. Bis zu acht Modemprofile können auf **X4100/200/300** im Menü ***MODEM*** ➧ ***PROFILE CONFIGURATION*** konfiguriert werden. Das tatsächlich genutzte Modem übernimmt beim Verbindungsaufbau jeweils dynamisch die Einstellungen des zugeordneten Modemprofils. Ein Modemprofil definiert die Einstellungen des Modems, die für eine Verbindung mit der Gegenstelle benötigt werden, z. B. automatische Baudraten-Aushandlung, Kompression oder maximale bzw. minimale Baudrate. Durch die Erstellung von mehreren Modemprofilen ergibt sich für Sie eine Tuning-Möglichkeit, wenn Sie nicht ausschließlich die Standardeinstellungen verwenden wollen.

Bei Festlegung der Einstellungen für Incoming Call Answering, z. B. im Menü ***CM-3BRI, ISDN S0, UNIT 0*** ➧ ***INCOMING CALL ANSWERING*** für die erste ISDN-BRI-Schnittstelle einer BRI-Erweiterungskarte (siehe "Incoming Call Answering", Seite 296), kann explizit definiert werden, welches Modemprofil für welche eigene Rufnummer verwendet werden soll. Ohne spezielle Zuweisung der Modemprofile an eigene Rufnummern verwendet das Modem des Routers automatisch **Modem Profile 1**.

Modem Profile 1 wird also als Standardeinstellung verwendet und sollte eine maximale Auswahl der Einstellungen zulassen. Da allen Dial-In-Usern, die nicht per CLID etc. authentisiert werden können, **Modem Profile 1** für die Verbindung zugewiesen wird, sollte **Modem Profile 1** alle Modems bedienen können. Mit den verbleibenden sieben Modemprofilen können Sie User-Gruppen definieren, so daß die einwählenden Dial-In-Verbindungspartner optimale Modemeinstellungen auf **X4100/200/300** vorfinden.

Beispielszenario

Ein typisches Szenario, z. B. für einen Internet Service Provider, könnte folgendermaßen aussehen:



Incoming Call Answering:

Number	Item
99	ISDN Login
50	PPP V.110
30	PPP (routing)
41	PPP Modem Profile 1
42	PPP Modem Profile 2
...	...

Bild 8-2: Szenario für Dial-In

- Eingehende Rufe an die Rufnummer 99 werden an den Dienst ISDN-Login weitergeleitet.

- Modemverbindugnen über 0911 12330 werden dem **Modem Profile 1** zugeweisen.
- Dial-In-User, die sich mit einem Handy über eine GSM-Verbindung einwählen, verwenden 0911 123 50.
- Dial-In-User, die eine ISDN-Verbindung nutzen, verwenden 0911 123 30.
- Dial-In-User, die sich über eine analoge Verbindung einwählen, benutzen zum Dial-In die Rufnummern 0911 123 41 bis 0911 123 48 (je nachdem, welchen analogen Modemtyp Sie verwenden).

Setup Tool mit Digitalmodems

Wenn **X4100/200/300** mit einer Ressourcenkarte mit Digitalmodems ausgestattet ist, erscheint das Menü ***MODEM*** im Setup-Tool-Hauptmenü:

```
X4x00 Setup Tool                              BinTec Access Networks GmbH
                                                                MyRouter

Licenses                  System

LAN:         CM-100BT,Fast Ethernet       Module:  X4E-3BRI,ISDN S0

WAN:         CM-1BRI,ISDN S0

Serial-WAN:  CM-SERIAL, Serial            Resources:XT-S

WAN Partner
IP      PPP      MODEM    ISDN     CAPI     QoS

Configuration Management
Monitoring and Debugging
Exit
```

Im Menü ***MODEM*** werden die Modemprofile, deren Einstellungen die Digitalmodems auf **X4100/200/300** nutzen, festgelegt.

Allgemeine Vorgehensweise bei der Konfiguration von Dial-In-Verbindungen:

- Die Einstellungen für das Standardmodemprofil **Modem Profile 1** in ***MODEM*** ➧ ***PROFILE CONFIGURATION*** definieren
- Gegebenenfalls weitere **Modem Profiles 2 ... 8** in ***MODEM*** ➧ ***PROFILE CONFIGURATION*** definieren

- Mit den Einstellungen für "Incoming Call Answering" die Verwendung der Modemprofile in Abhängigkeit von der gerufenen Nummer regeln (z. B. in ***X4E-3BRI, ISDN S0*** ➧ ***UNIT 0*** ➧ ***INCOMING CALL ANSWERING***)
- Für jeden Dial-In-User einen WAN-Partner-Eintrag in ***WAN PARTNER*** konfigurieren

Die Menüs ***MODEM*** ➧ ***PROFILE CONFIGURATION*** ➧ ***PROFILE 1 ... 8*** enthalten folgende Felder:

Feld	Bedeutung
Name	Profile 1 ... 8 wird angezeigt.
Description	Frei wählbare Beschreibung des Modemprofils.
Modulation	Legt den zu benutzenden Modemstandard fest (im Auslieferungszustand V.34). Der gewählte Modemstandard muß vom analogen Modem der Gegenstelle unterstützt werden. *V.90* und niedrigere Werte werden von 56000er-Modems unterstützt, *V.34* und niedrigere Werte von 33600er-Modems, *V.32bis* und niedrigere Werte von 14400er-Modems. Mögliche Werte: ■ *V.90* ■ *k56flex* ■ *V.34* ■ *V.32bis* ■ *V.32* Weitere Modemstandards sind in Vorbereitung. Den Stand der Implementierung können Sie unter www.X4000.de verfolgen.
Error Correction	Legt die zu benutzende Fehlerkorrektur fest. Mögliche Werte siehe Tabelle 8-3, Seite 307.

Feld	Bedeutung
Automode	Legt fest, ob die dynamische Aushandlung der Modulation mit dem Dial-In-User erlaubt ist. Mögliche Werte: ■ *on* (Standardwert): freie Aushandlung, unabhängig von der eingestellten Modulation, ist erlaubt. ■ *off*: Es wird nur die eingestellte Modulation verwendet.
Min Bps	Legt die minimale Baudrate fest, die mit dem Modemprofil genutzt werden kann. Jede Geschwindigkeit, die von dem unter **Modulation** eingestellten Modemstandard unterstützt wird, kann hier eingestellt werden. Die Verbindung wird abgebaut, wenn mit der Gegenstelle nur eine Baudrate ausgehandelt werden kann, die kleiner als der hier eingestellte Wert ist. Skalierbar von *75* bis *56000,* Standardwert: *300*.
Max Receive Bps	Legt die maximale Baudrate für eingehende Daten fest, die mit dem Modemprofil genutzt werden kann. Jede Geschwindigkeit, die von dem unter **Modulation** eingestellten Modemstandard unterstützt wird, kann hier eingestellt werden. Der unter **Max Transmit Bps** eingestellte Wert wird hier verwendet, falls dieser Wert kleiner ist als der hier eingestellte. Skalierbar von *75* bis *56000*, Standardwert: *33600*.

Feld	Bedeutung
Max Transmit Bps	(Nur verwendet wenn **Modulation** = *V.90*.) Legt die maximale Baudrate für ausgehende Daten ("downstream") fest, die mit dem Modemprofil genutzt werden kann. Skalierbar von *75* bis *56000*, Standardwert: *33600*.
V.42bis Compression	Legt fest, ob V.42bis-Kompression für eine Verbindung ausgehandelt werden darf. Mögliche Werte: ■ *auto*: Aushandlung wird erlaubt. ■ *off*: V.42bis-Kompression wird nicht genutzt.
MNP5 Compression	Legt fest, ob MNP5-Kompression für eine Verbindung ausgehandelt werden darf. Mögliche Werte: ■ *auto*: Aushandlung wird erlaubt. ■ *off*: MNP5-Kompression wird nicht genutzt.

Tabelle 8-2: Menü ***MODEM*** ➧ ***PROFILE CONFIGURATION*** ➧ ***PROFILE 1 ... 8***

Das Feld **Error Correction** enthält folgende Auswahlmöglichkeiten:

Mögliche Werte	Bedeutung
none	Fehlerkorrektur wird nicht genutzt.
required	Als Fehlerkorrektur wird zunächst LAPM und anschließend MNP4 versucht. Schlägt beides fehl, beendet das Modem die Verbindung.
auto (Standardwert)	Als Fehlerkorrektur wird zunächst LAPM und anschließend MNP5 versucht. Schlägt beides fehl, wird keine Fehlerkorrektur genutzt.

Mögliche Werte	Bedeutung
LAPM	LAPM (Link Access Protocol for Modems) wird genutzt. Wenn dies fehlschlägt, beendet das Modem die Verbindung.
MNP	MNP4 (Microcom Networking Protocol) wird genutzt. Wenn dies fehlschlägt, beendet das Modem die Verbindung.

Tabelle 8-3: **Error Correction**

Modem Profile 1 konfigurieren

Gehen Sie folgendermaßen vor:

Modem Profile 1 wird als Standardeinstellung für Modemverbindungen verwendet und sollte eine maximale Auswahl der Einstellungen zulassen. Da allen Dial-In-Usern, die nicht per CLID etc. authentisiert werden können, **Modem Profile 1** für die Verbindung zugewiesen wird, sollte **Modem Profile 1** alle Modems bedienen können.

- Gehen Sie zu ***MODEM*** ➧ ***PROFILE CONFIGURATION***.
- Wählen Sie ***PROFILE 1*** aus und bestätigen mit der **Eingabetaste**.
- Geben Sie **Description** ein, z. B. ***Standardmodemprofil***.
- Wählen Sie **Modulation** aus, z. B. ***V.90***.
- Wählen Sie **Error Correction** aus, z. B. ***auto***.
- Wählen Sie **Automode** aus, z. B. ***on***.
- Wählen Sie **V.42bis Compression** aus, z. B. ***auto***.
- Wählen Sie **MNP5 Compression** aus, z. B. ***auto***.
- Bestätigen Sie mit **SAVE**.

Modem Profile 2 ... 8 konfigurieren

- Konfigurieren Sie gegebenenfalls weitere Modemprofile. Beachten Sie dabei Tabelle 8-4, Seite 309.

Incoming Call Answering

Gehen Sie folgendermaßen vor, um die definierten Modemprofile den eigenen Rufnummern zuzuordnen (die Beispielwerte sind dem Szenario in Bild 8-2, Seite 302 entnommen):

- Gehen Sie zu ***X4E-3BRI, ISDN S0*** ➧ ***UNIT 0*** ➧ ***INCOMING CALL ANSWERING***, wenn Sie eine – über die erste Schnittstelle einer ISDN-BRI-Erweiterungskarte eingehende – Dial-In-Verbindung einem Modemprofil zuordnen möchten.
- Fügen Sie mit **ADD** einen neuen Eintrag hinzu.
- Wählen Sie **Item** aus, z. B. ***PPP Modem Profile 2***.
- Geben Sie **Number** ein, z. B. ***42***.
- Wählen Sie **Mode** aus, z. B. ***right to left***.
- Wählen Sie **Bearer** aus, z. B. ***voice***.
- Bestätigen Sie mit **SAVE**.
- Fügen Sie gegebenenfalls weitere Einträge hinzu.

WAN-Partner-Einträge für Modem-User

Gehen Sie folgendermaßen vor, um für die Modem-User WAN-Partner-Einträge zu erzeugen:

- Gehen Sie zu ***WAN PARTNER***, fügen Sie mit **ADD** einen neuen Eintrag hinzu.
  Detaillierte Informationen zur Einrichtung eines WAN-Partners finden Sie in Kapitel 6.3, Seite 147, folgende Einstellungen sind hier auf jeden Fall erforderlich:
- Geben Sie **Partner Name** ein, z. B. ***homeoffice_2***.
- Wählen Sie **Encapsulation** aus, z. B. ***PPP***.
- Wählen Sie Authentisierungsinformationen in ***WAN PARTNER*** ➧ ***ADD*** ➧ ***PPP*** aus.
- Gehen Sie zu ***WAN PARTNER*** ➧ ***ADD*** ➧ ***ADVANCED SETTINGS***.
- Wählen Sie **Layer 1 Protocol** aus, z. B. ***Modem Profile 2***.
- Bestätigen Sie mit **OK**.
- Gehen Sie zu ***WAN PARTNER*** ➧ ***ADD*** ➧ ***WAN NUMBERS*** ➧ ***ADD***.

- Geben Sie unter **Number** die von **X4100/200/300** zu verwendende Rufnummer ein, z B. ***09117890***.
- Wählen Sie **Direction** aus, z. B. ***both (CLID)***.
- Bestätigen Sie mit **SAVE**.
- Verlassen Sie ***WAN PARTNER*** ➧ ***ADD*** ➧ ***WAN NUMBERS*** mit **EXIT**.
- Wählen Sie die erforderlichen Einstellungen in ***WAN PARTNER*** ➧ ***ADD*** ➧ ***IP*** (siehe "IP-Konfiguration durchführen", Seite 163).
- Bestätigen Sie mit **SAVE**.

  Der WAN-Partner-Eintrag wird angezeigt.
- Konfigurieren Sie gegebenenfalls weitere WAN-Partner-Einträge für die Modem-User.

Anhand eines allgemeines Beispiels zeigt Tabelle 8-4, Seite 309, wie Sie die Modemprofile auf **X4100/200/300** auf sinnvolle Weise nutzen könnten:

Profile	Modulation	Error Correction	Automode	Min Bps	Max Receive Bps	Max Transmit Bps	v.42bis	MNP5
Profile 1	*(Modulation wird frei ausgehandelt)*	*auto*	*on*	*2400*	*33600*	*33600*	*auto*	*auto*
Profile 2	*V.90*	*auto*	*off*	*28800*	*31200*	*50000*	*auto*	*auto*
Profile 3	*V.90*	*auto*	*off*	*28800*	*31200*	*44000*	*auto*	*auto*
Profile 4	*V.90*	*auto*	*off*	*14400*	*31200*	*40000*	*auto*	*auto*
Profile 5	*V.32bis*	*auto*	*off*	*4800*	*14400*	*14400*	*auto*	*auto*
Profile 6	*V.32*	*auto*	*off*	*4800*	*9600*	*9600*	*auto*	*auto*
Profile 7	*V.23*	*auto*	*off*	*300*	*1200*	*1200*	*auto*	*auto*

Tabelle 8-4: Beispiele für Modemprofile

8.5 Ressourcenkarte zur Verschlüsselung und Kompression

Die ISDN-PRI- bzw. G.703-Erweiterungskarte ist im Auslieferungszustand mit Hardware-Unterstützung für Verschlüsselung und Kompression ausgestattet. Die ISDN-BRI-Erweiterungskarte sowie die LAN-Erweiterungskarte kann optional mit einer entsprechenden Ressourcenkarte ausgestattet werden.

Eine Ressourcenkarte zur Verschlüsselung und Kompression unterstützt STAC-Kompression und symmetrische Verschlüsselungsverfahren (DES, 3DES, CAST, Blowfish). Somit kann die zur Verfügung stehende Bandbreite maximal ausgenutzt und die Verbindungskosten gesenkt werden, ohne die Performanz von **X4100/200/300** zu beeinträchtigen.

Achtung!

Der Einbau der PRI/G.703-Erweiterungskarte bzw. der Einbau von Ressourcenkarten in eine Erweiterungskarte führt zu verstärkter Wärmeentwicklung. Um die Schädigung von Bauteilen zu vermeiden, ist der Einsatz einer Lüfterkassette zwingend erforderlich!

- Setzen Sie bei Verwendung der PRI/G.703-Erweiterungskarte oder einer Erweiterungskarte mit Ressourcenkarte(n) im **X4100/200/300**-Einbaugerät die Lüfterkassette ein.

Sie können die Lüfterkassette von Ihrem Lieferanten käuflich erwerben.

Konfiguration mit dem Setup Tool

Die Konfiguration von STAC-Kompression und Verschlüsselung erfolgt im Setup-Tool-Menü ***WAN PARTNER*** ➧ ***EDIT*** (siehe Kapitel 7.2.10, Seite 222 bzw. Kapitel 9.3.1, Seite 362).

9 Konfiguration von Sicherheitsfunktionen

SAFERNET

BinTec Access Networks GmbH ermöglicht mit **X4100/200/300** eine hohe Sicherheit Ihres Netzwerks und Ihrer Verbindungen. Die verfügbaren Sicherheitsfunktionen (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. **Configuration Manager**, vornehmen. Eine Beschreibung der SNMP-Kommandos finden Sie in der **Software Reference**.

Das Kapitel ist folgendermaßen aufgebaut:

9.1 Überwachen von Aktivitäten

Eine wesentliche Voraussetzung für einen hohen Grad an Sicherheit ist die Möglichkeit, alle Aktivitäten auf dem Router und über den Router hinweg exakt beobachten zu können. Dazu stellt Ihnen BinTec Access Networks GmbH eine Vielzahl an Möglichkeiten zur Verfügung:

- Syslog-Messages (Kapitel 9.1.1, Seite 312)
- Monitorfunktionen im Setup Tool (Kapitel 9.1.2, Seite 317)
- Credits Based Accounting System (Taschengeldkonto) (Kapitel 9.1.3, Seite 321)
- **Activity Monitor** (Kapitel 9.1.4, Seite 325)

9.1.1 Syslog-Messages

Alle wesentlichen Ereignisse auf **X4100/200/300**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 intern auf **X4100/200/300** 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 Systemadministrators. Auf **X4100/200/300** intern gespeicherte Syslog-Messages gehen 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***
- ***CM-100BT, FAST ETHERNET*** ➧ ***ADVANCED SETTINGS***
- ***WAN PARTNER*** ➧ ***EDIT*** ➧ ***IP*** ➧ ***ADVANCED SETTINGS***

Menü ***SYSTEM***:

Feld	Bedeutung
Syslog output on serial console	Ermöglicht die Anzeige von Syslog-Messages auf dem mit der seriellen Schnittstelle von **X4100/200/300** verbundenen Rechner. Verwenden Sie diese Einstellung nur, wenn Sie eine Fehleranalyse machen, da massiver Output über die serielle Konsole sich auf den Durchsatz der anderen Schnittstellen auswirkt. Mögliche Werte: ■ *yes* ■ *no*

Feld	Bedeutung
Message level for the syslog table	Spezifiziert die Priorität der intern aufzuzeichnenden Syslog-Messages. Mögliche Werte: ■ *emerg*: Emergency Messages (höchste Priorität) ■ *alert*: Alert Messages ■ *crit*: Critical Messages ■ *err*: Error Messages ■ *warning*: Warning Messages ■ *notice*: Notice Messages ■ *info*: Info Messages ■ *debug*: Debug Messages (niedrigste Priorität) Nur Syslog-Messages mit höherer oder gleicher Priorität als angegeben werden intern aufgezeichnet.
Maximum Number of Syslog Entries	Maximale Anzahl an Syslog-Messages, die auf **X4100/200/300** intern gespeichert werden (Wertebereich: *0* ... *100*).

Tabelle 9-1: ***SYSTEM***

Menü ***SYSTEM*** ➧ ***EXTERNAL SYSTEM LOGGING***:

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.

Feld	Bedeutung
Type	Nachrichtentyp. Mögliche Werte: ■ *all*: Alle Messages. ■ *system*: Syslog-Messages außer ➤➤ **Accounting**-Messages. ■ *accounting*: Accounting-Messages.
Timestamp	Systemzeit von **X4100/200/300**. Mögliche Werte: ■ *all*: Systemzeit mit Datum ■ *time*: Systemzeit ohne Datum ■ *none*: keine Systemzeitangabe

Tabelle 9-2: ***System*** ➧ ***External System Logging***

Menü ***CM-100BT, Fast Ethernet*** ➧ ***Advanced Settings***:

Feld	Bedeutung
IP Accounting	Ermöglicht Speichern von Accounting-Messages für ➤➤ **TCP**-, ➤➤ **UDP**- und ICMP-Sitzungen. Mögliche Werte: *on*, *off*.

Tabelle 9-3: ***CM-100BT, Fast Ethernet*** ➧ ***Advanced Settings***

Menü ***WAN Partner*** ➧ ***Edit*** ➧ ***IP*** ➧ ***Advanced Settings***:

Feld	Bedeutung
IP Accounting	Ermöglicht Speichern von Accounting-Messages für ➤➤ **TCP**-, ➤➤ **UDP**- und ICMP-Sitzungen. Mögliche Werte: *on*, *off*.

Tabelle 9-4: ***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 den gewünschten Wert für **Syslog output on serial console** aus.
- Wählen Sie den gewünschten Wert für **Message level for the syslog table** aus.
- Geben Sie den gewünschten Wert für **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 den gewünschten Wert für **Level** aus.
- Wählen Sie den gewünschten Wert für **Facility** aus.
- Wählen Sie den gewünschten Wert für **Type** aus.

IP-Accounting LAN-seitig Gehen Sie folgendermaßen vor, um IP-Accounting für einen LAN-Partner zu aktivieren. Damit werden auf **X4100/200/300** Accounting-Messages von TCP-, UDP- und ICMP-Sitzungen bezüglich des ausgewählten LAN-Partners generiert und aufgezeichnet:

- Gehen Sie zu ***CM-100BT, Fast Ethernet*** ➧ ***Advanced Settings***.
- Aktivieren Sie **IP Accounting** mit *on*.

IP-Accounting WAN-seitig Gehen Sie folgendermaßen vor, um erweitertes IP-Accounting zu aktivieren. Damit werden auf **X4100/200/300** Accounting-Messages von TCP-, UDP- und ICMP-Sitzungen bezüglich des ausgewählten WAN-Partners generiert und aufgezeichnet:

- 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 **X4100/200/300** intern gespeicherten Syslog-Messages angezeigt:

```
X4x00 Setup Tool                          BinTec Access Networks GmbH
[MONITOR][MESSAGE]: Syslog Messages                            MyRouter

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


EXIT        RESET

Press <Ctrl-n>, <Ctrl-p> to scroll
```

Löschen von Syslog-Messages

➤ Wählen Sie **RESET**, um die Syslog-Messages auf **X4100/200/300** zu löschen.

Zur Interpretation von Syslog-Messages: Siehe **Software Reference**.

9.1.2 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 Anzeigemodule:

- ISDN-Verbindungen
- Taschengeldkonto
- Schnittstellenstatistik (vergleichende Darstellung mehrerer Schnittstellen)
- ➤➤ **TCP/IP**-Statistik
- Syslog-Messages (siehe Kapitel 9.1.1, Seite 312)

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:

```
X4x00 Setup Tool                          BinTec Access Networks GmbH
[MONITOR][ISDN CALLS]: ISDN Monitor - Calls                   MyRouter

Dir Remote Name/Number   Charge   Duration    Stack   Channel  State

in  2                             2910        0       B1       active
out 3                             106         0       B2       active



(c)alls    (h)istory    (d)etails    (s)tatistics    (r)elease
```

Weitere Optionen stehen Ihnen in diesem Menü zur Verfügung:

➤ Wählen Sie `c`, um wieder die Liste der bestehenden ISDN-Verbindungen anzuzeigen.

➤ 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 `r`, um die markierte ISDN-Verbindung zu schließen.

Taschengeldkonto für ISDN-Verbindungen

Gehen Sie folgendermaßen vor, um den Stand des Taschengeldkontos (Kapitel 9.1.3, Seite 321) 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:

```
X4x00 Setup Tool                          BinTec Access Networks GmbH
[MONITOR][CREDITS][STAT]: Monitor isdnlogin Credits          MyRouter


                                          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              4        28800    0
Time of Outgoing Connections              13       28800    0

Charge                                    0

Number of Current Incoming Connections    0
Number of Current Outgoing Connections    0
Number of Current Connections             0

EXIT
```

Informationen über die Konfiguration des Taschengeldkontos finden Sie in Kapitel 9.1.3, Seite 321.

Taschengeldkonto für PPPoE-Verbindungen

Gehen Sie folgendermaßen vor, um den Stand des Taschengeldkontos für PPPoE-Verbindungen anzeigen zu lassen:

➤ Gehen Sie zu ***Monitoring and Debugging*** ➧ ***xDSL Credits*** ➧ ***PPPoE Credits***.

Der aktuelle Stand des Taschengeldkontos für PPPoE-Verbindungen wird angezeigt.

Schnittstellenstatistik

Gehen Sie folgendermaßen vor, um aktuelle Werte und Aktivitäten der **X4100/200/300**-Schnittstellen anzuzeigen:

➤ Gehen Sie zu ***Monitoring and Debugging*** ➧ ***Interfaces***.

Die Werte von zwei Schnittstellen werden nebeneinander angezeigt:

```
X4x00 Setup Tool                              BinTec Access Networks GmbH
[MONITOR][INTERFACE]: Interface Monitoring                        MyRouter

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.

```
X4x00 Setup Tool                                BinTec Access Networks GmbH
[MONITOR][IP]: IP Statistics                                      MyRouter

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
```

Die Bedeutung der MIB-Variablen finden Sie in der **MIB Reference**.

- Wählen Sie `C`, um statische Daten zu ICMP darzustellen.
- Wählen Sie `I`, um statische Daten zu IP darzustellen.
- Wählen Sie `U`, um statische Daten zu UDP darzustellen.
- Wählen Sie `T`, um statische Daten zu ICMP darzustellen.

9.1.3 Credits Based Accounting System (Taschengeldkonto)

ISDN-Gebühren

Mit dem Taschengeldkonto von **X4100/200/300** übernehmen Sie die Kontrolle über anfallende ISDN-Gebühren für Datenverbindungen. Dadurch können Sie die Auswirkungen eventueller Konfigurationsfehler in Grenzen halten. Es ermöglicht Ihnen u. a. 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 **X4100/200/300** 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 die Taschengeldkonto-Funktion wegen überschrittenem Limits eine Verbindung verhindert.

Nach Aus- und wieder Einschalten bzw. Rebooten von **X4100/200/300** steht Ihnen wieder das gesamte Konto zur Verfügung.

Die Konfiguration erfolgt in ***ISDN*** ➧ ***ISDN CREDITS*** bzw. in ***ISDN*** ➧ ***xDSL CREDITS*** ➧ ***PPPoE CREDITS***:

Die Felder für eingehende Verbindungen stehen nur für ISDN zur Verfügung.

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 Gebühren (Betrag, Einheiten) 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 Incoming Connections (sec)	Maximal erlaubte Zeit 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.
Maximum Time for Outgoing Connections (sec)	Maximal erlaubte Zeit 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.
Maximum Number of Current Incoming Connections	Maximale Anzahl der zu einem Zeitpunkt gleichzeitig erlaubten eingehenden Verbindungen. Wenn Sie diese Einstellung mit *on* aktivieren, können Sie den gewünschten Wert in der darunterliegenden Zeile eintragen.
Maximum Number of Current Outgoing Connections	Maximale Anzahl der zu einem Zeitpunkt gleichzeitig erlaubten ausgehenden Verbindungen. Wenn Sie diese Einstellung mit *on* aktivieren, können Sie den gewünschten Wert in der darunterliegenden Zeile eintragen.

Tabelle 9-5: ***ISDN*** ➧ ***ISDN CREDITS*** ➧ bzw. ***ISDN*** ➧ ***xDSL CREDITS*** ➧ ***PPPoE CREDITS***

ToDo Gehen Sie folgendermaßen vor:

- Gehen Sie zu ***ISDN*** ➧ ***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 den gewünschten Wert ein.
- Aktivieren Sie gegebenenfalls **Maximum Number of Outgoing Connections** und tragen Sie den gewünschten Wert ein.
- Aktivieren Sie gegebenenfalls **Maximum Charge** und tragen Sie den gewünschten Wert ein.
- Aktivieren Sie gegebenenfalls **Maximum Time for Incoming Connections (sec)** und tragen Sie den gewünschten Wert ein.
- Aktivieren Sie gegebenenfalls **Maximum Time for Outgoing Connections (sec)** und tragen Sie den gewünschten Wert ein.
- Aktivieren Sie gegebenenfalls **Maximum Number of Current Incoming Connections** und tragen Sie den gewünschten Wert ein.
- Aktivieren Sie gegebenenfalls **Maximum Number of Current Outgoing Connections** und tragen Sie den gewünschten Wert ein.
- Bestätigen Sie mit **SAVE**.

  Das Taschengeldkonto für ISDN-Verbindungen ist eingerichtet.

Gehen Sie folgendermaßen vor, um ein Taschengeldkonto für PPPoE-Verbindungen einzurichten:

- Gehen Sie zu ***ISDN*** ➧ ***xDSL CREDITS*** ➧ ***PPPOE CREDITS***.
- Wählen Sie **Surveillance** aus: *on*, wenn Sie das Taschengelkonto nutzen wollen.
- Geben Sie **Measure Time (sec)** ein, z. B. ***86400*** (=24 Stunden).
- Aktivieren Sie gegebenenfalls **Maximum Number of Outgoing Connections** und tragen Sie den gewünschten Wert ein.
- Aktivieren Sie gegebenenfalls **Maximum Time for Outgoing Connetions (sec)** und tragen Sie den gewünschten Wert ein.
- Bestätigen Sie mit **SAVE**.

  Das Taschengeldkonto für PPPoE-Verbindungen ist eingerichtet.

9.1.4 Activity Monitor

Wozu? Mit dem **Activity Monitor** können Windows-Nutzer die Aktivitäten von **X4100/200/300** überwachen. Wichtige Informationen über den Status von physikalischen Schnittstellen (z. B. ISDN-Leitung) und virtuellen Schnittstellen (z. B. WAN-Partner) sind leicht mit einem Tool erreichbar. Ein permanenter Überblick über die Auslastung der Schnittstellen von **X4100/200/300** ist möglich.

Wie funktioniert's? Ein Status-Daemon sammelt Informationen über **X4100/200/300** und überträgt sie in Form von UDP-Paketen zur Broadcast-Adresse des LAN (Standardeinstellung) oder zu einer explizit eingetragenen IP-Adresse. Ein Paket pro **X4100/200/300**-Schnittstelle und Zeitintervall, das individuell einstellbar ist auf Werte von 1 - 60 Sekunden, wird gesendet. Alle physikalischen Schnittstellen und bis zu 100 virtuelle Schnittstellen können überwacht werden, soweit die Paket-Größe von ca. 4000 Bytes nicht überschritten wird. Eine Windows-Anwendung auf Ihrem PC, die mit dem BRICKware Release 5.1.1 und höher erhältlich ist, empfängt die Pakete und stellt die enthaltenen Informationen auf verschiedene Arten dar.

Um den **Activity Monitor** zu aktivieren, müssen Sie:

- die zu überwachenden **X4100/200/300**(s) entsprechend konfigurieren
- die Windows-Anwendung auf Ihrem PC starten und verwenden (siehe **BRICKware for Windows**)

Die Konfiguration erfolgt in ***System*** ➧ ***External Activity Monitor***:

Feld	Bedeutung
Client IP Address	IP-Adresse, zu der **X4100/200/300** die UDP-Pakete schickt. Mit dem Standardwert *255.255.255.255* wird die Broadcast-Adresse der ersten LAN-Schnittstelle verwendet. Beachten Sie: Wenn Sie hier die IP-Adresse eines WAN-Partners eingeben, der über eine ISDN-Wahlverbindung erreichbar ist, entstehen Ihnen hohe Kosten durch häufiges Aufbauen von ISDN-Verbindungen (im Auslieferungszustand wird alle 5 Sekunden ein Paket geschickt).
Client UDP Port	Port-Nummer für Activity Monitor (Standardwert: *2107*, registriert durch IANA - Internet Assigned Numbers Authority).
Type	Art der Informationen, die mit den UDP-Paketen zur Windows-Anwendung geschickt werden. Mögliche Werte: ■ *off:* deaktiviert **Activity Monitor** (Standardwert) ■ *physical:* nur Informationen über physikalische Schnittstellen ■ *physical_virt:* Informationen über physikalische und virtuelle Schnittstellen
Update Interval (sec)	Update-Intervall in Sekunden. Mögliche Werte: *0* bis *60* (Standardwert: *5*).

Tabelle 9-6: ***System*** ➧ ***External Activity Monitor***

Die Einteilung der **X4100/200/300**-Schnittstellen in physikalische und virtuelle Schnittstellen finden Sie in der **Software Reference** genau beschrieben.

Beachten Sie: Eine Festverbindung stellt immer eine physikalische Schnittstelle dar. Aber ein Bündel von Festverbindungen wird sowohl als physikalische, als auch als virtuelle Schnittstelle angezeigt!

ToDo Gehen Sie folgendermaßen vor:

- Gehen Sie zu ***System*** ➧ ***External Activity Monitor***.
- Geben Sie **Client IP Address**, **Client UDP port**, **Type** und **Update Interval (sec)** ein.
- Bestätigen Sie mit **SAVE**.

9.2 Zugangssicherung

Es gibt einige Möglichkeiten, das Einloggen und Zugreifen auf **X4100/200/300** nur autorisierten Benutzern zu ermöglichen:

- Anmelden (Kapitel 9.2.1, Seite 328)
- Überprüfen der eingehenden Rufnummer (CLID) (Kapitel 9.2.2, Seite 329)
- Authentisierung von PPP-Verbindungen (Kapitel 9.2.3, Seite 330)
- Callback (Kapitel 9.2.4, Seite 331)
- Closed User Group (Kapitel 9.2.5, Seite 333)
- Zugriff auf Remote-CAPI (Kapitel 9.2.6, Seite 333)
- Network Address Translation (NAT) (Kapitel 9.2.7, Seite 334)
- Filter (Kapitel 9.2.8, Seite 339)
- Lokale Filter (Kapitel 9.2.9, Seite 351)
- Backroute Verification (Kapitel 9.2.10, Seite 356)
- TAF (Kapitel 9.2.11, Seite 356)
- Extended IP-Routing (XIPR) (Kapitel 9.2.12, Seite 357)

9.2.1 Anmelden

Paßwort

Das Anmelden auf **X4100/200/300** kann, wie in Kapitel 4.2, Seite 62 beschrieben, über mehrere Wege erfolgen, ist aber immer paßwortgesichert. Jeder Fehlversuch wird mit Angabe der Quelle per Syslog-Messages 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 unautorisierten Zugriff geschützt, solange die Paßwörter nicht geändert wurden. Die Vorgehensweise bei der Änderung von Paßwörtern ist unter Kapitel 4.4.4, Seite 71 beschrieben.

- Ändern Sie unbedingt die Paßwörter wie in Kapitel 4.2, Seite 62 beschrieben.
- Achten Sie zusätzlich darauf, daß Unbefugte nicht auf die Stromzufuhr zu **X4100/200/300**, 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 eine Warnung ausgegeben.

Autologout

Um unberechtigte Zugriffe zu erschweren, wird die Verbindung zu **X4100/200/300** 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 13.1, Seite 418).

Wenn Sie ein Software-Update durchführen (siehe Kapitel 10.2, Seite 382), sollten Sie den Autologout ausschalten: Geben Sie `t 0` in die SNMP-Shell ein.

Es ist möglich, zusätzliche Benutzer-Accounts mit Hilfe von SNMP-Kommandos anzulegen (siehe **Software Reference**). Einem Benutzer kann dabei ein bestimmtes Paßwort und eine bestimmte Aktion zugeordnet werden.

9.2.2 Überprüfen der eingehenden Rufnummer

CLID

Mit Hilfe von Calling Line Identification (➤➤ **CLID**) überprüft **X4100/200/300** die Calling Party's Number eines eingehenden Rufes.

Screening-Indikator

Darüber hinaus 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 **X4100/200/300** 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).

Variable Screening ändern in MIB

Wenn **X4100/200/300** bei eingehenden Rufen den Screening-Indikator überprüfen soll, müssen Sie einen der genannten Werte in die 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**.

Zum Ändern von MIB-Variablen siehe Kapitel 4.3, Seite 64.

9.2.3 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 6.3, Seite 147 und Kapitel 7.1.3, Seite 186.

9.2.4 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. **X4100/200/300** 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 9-7: ***WAN Partner*** ➧ ***Edit*** ➧ ***Advanced Settings***

Callback enthält folgende Auswahlmöglichkeiten:

Mögliche Werte	Bedeutung
no	**X4100/200/300** führt keinen Rückruf aus.
expected (awaiting callback)	**X4100/200/300** ruft den WAN-Partner an, um den Callback zu initiieren.

Mögliche Werte	Bedeutung
yes (PPP negotiation)	**X4100/200/300** 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, CLID only)	**X4100/200/300** ruft nach ca. vier Sekunden zurück, wenn Ihr Router vom WAN-Partner dazu aufgefordert wird.
yes (PPP negotiaton, callback optional)	Wie *yes (PPP negotiation)* mit Abbruchoption. Der Microsoft-Client hat hier die Möglichkeit, den Callback abzubrechen und die initiale Verbindung zu **X4100/200/300** ohne Callback aufrechtzuerhalten. Dies wird erreicht, indem das erscheinende Dialogfenster mit **CANCEL** geschlossen wird. Ausnahme: Wenn der einwählende WAN-Partner Windows NT nutzt und seine Rufnummer auf **X4100/200/300** eingetragen ist, kann diese Abbruchoption nicht genutzt werden!
yes	**X4100/200/300** ruft sofort zurück, wenn Ihr Router vom WAN-Partner dazu aufgefordert wird.

Tabelle 9-8: **Callback**

Bei der Einstellung *yes (PPP negotiation)* für **Callback** wird immer ein B-Kanal geöffnet, wodurch Kosten verursacht werden.

ToDo Gehen Sie folgendermaßen vor, um Callback für einen WAN-Partner zu aktivieren:

- Gehen Sie zu ***WAN Partner*** ➧ ***Edit*** ➧ ***Advanced Settings***.
- Wählen Sie den gewünschten Wert für **Callback** aus.
- Bestätigen Sie mit **OK**.

9.2.5 Closed User Group

X4100/200/300 unterstützt die Nutzung des Dienstmerkmals "Geschlossene Benutzergruppe", das Sie bei Ihrer Telefongesellschaft für Ihren ISDN-Anschluß beantragen können. Damit wird die externe/interne Erreichbarkeit durch die Vermittlungsstellen überwacht und geregelt.

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 CUG-Index ein.
  Informationen zu CUG erhalten Sie von Ihrer Telefongesellschaft.
- Bestätigen Sie mit **OK**.

9.2.6 Zugriff auf Remote-CAPI

Zu den Besonderheiten der BinTec-Router gehört die Implementierung der Programmierschnittstellen ➧➧ **Remote-CAPI** und bei PABX-Geräten Remote-TAPI. Dadurch können Applikationen auf Rechnern im LAN die Ressourcen des Routers nutzen, so als wären diese Komponenten direkt im Rechner eingebaut.

User Concept Durch Nutzung von BinTecs User Concept können Sie sicherstellen, daß nur durch Benutzername und Paßwort authentisierte Benutzer auf die Remote-CAPI-Schnittstelle von **X4100/200/300** zugreifen können (siehe Bild 6-3, Seite 127).

Filter Mit der Definition von Filtern (siehe Kapitel 9.2.8, Seite 339) und lokalen Filtern (siehe Kapitel 9.2.9, Seite 351) können Sie unbefugten Zugriff ebenfalls verhindern.

9.2.7 NAT (Network Address Translation)

➤➤ **NAT** ist ein einfach zu bedienendes Verfahren, das in der Implementierung von BinTec zu mehreren Zwecken benutzt werden kann:

- Verbergen der internen Host-Adressen eines LANs durch Ummappen auf eine oder mehrere externe Adressen.
- Regelung des Zugangs von extern nach intern. Nach extern leitet der Router alle ➤➤ **Datenpakete** weiter (Forward NAT). Verbindungen von extern werden dagegen nur bei expliziter Freigabe zugelassen.
- Permanente Überwachung der Verbindungen über den Router mit Quell- und Zielangabe der Adressen und ➤➤ **Ports**. Beachten Sie hierzu Ihre Syslog-Messages!

Grafische Darstellung von Forward NAT:

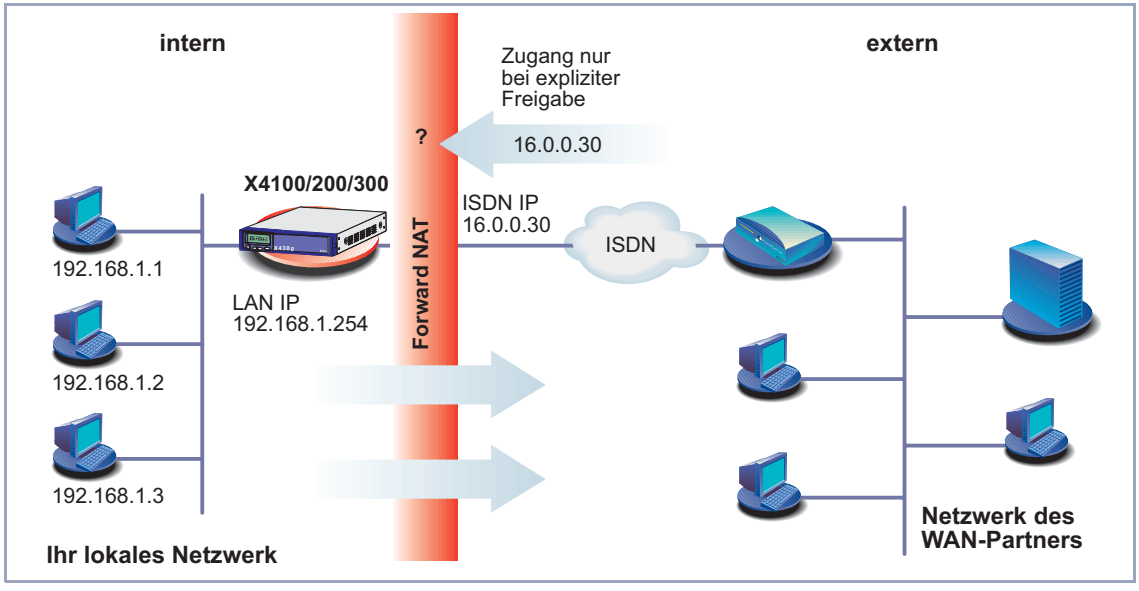


Bild 9-1: Forward NAT

NAT bezieht sich immer auf eine Schnittstelle. **X4100/200/300**s LAN-Seite wird dabei immer als "intern" bezeichnet, der WAN-Partner befindet sich "extern".

Weitere Erklärungen zu NAT finden Sie in der **Software Reference**.

Die Konfiguration erfolgt in ***IP*** ➧ ***NETWORK ADDRESS TRANSLATION***.

In ***IP*** ➧ ***NETWORK ADDRESS TRANSLATION*** sind alle Schnittstellen von **X4100/200/300** mit einer Statusanzeige für aktuelle NAT-Einstellungen aufgelistet:

Feld	Bedeutung
Name	Name der Schnittstelle.

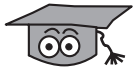
Feld	Bedeutung
Nat	Zeigt an, ob NAT für die entsprechende Schnittstelle aktiviert ist. Mögliche Werte: ■ *off*: Kein NAT aktiviert. ■ *on*: Forward NAT aktiviert. ■ *reverse*: Reverse NAT aktiviert
static mappings	Zeigt bei **Nat** = *on* bzw. **Nat** = *reverse* die Anzahl von Einträgen an, die für die Schnittstelle zur Freigabe von bestimmten IP-Verbindungen unter ***IP*** ➧ ***NETWORK ADDRESS TRANSLATION*** ➧ **Eingabetaste** ➧ **ADD** gemacht wurden.

Tabelle 9-9: ***IP*** ➧ ***NETWORK ADDRESS TRANSLATION***

In ***IP*** ➧ ***NETWORK ADDRESS TRANSLATION*** ➧ **EDIT** aktivieren Sie NAT für eine Schnittstelle von **X4100/200/300**:

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 9-10: ***IP*** ➧ ***NETWORK ADDRESS TRANSLATION*** ➧ **Eingabetaste**



Reverse NAT ist vor allem für Systemadministratoren von Interesse, die z. B. NAT für einen WAN-Partner übernehmen wollen, der dies nicht selbst durchführen kann. Hierbei verbirgt **X4100/200/300** nicht automatisch das lokale Netzwerk hinter der vom Service Provider zugewiesenen globalen IP-Adresse. Um dasselbe Maß an Sicherheit zu gewährleisten, ist ein erhöhter Konfigurationsaufwand erforderlich.

In ***IP*** ➧ ***NETWORK ADDRESS TRANSLATION*** ➧ ***EDIT*** ➧ **ADD** können Sie an einer NAT-Schnittstelle bestimmte IP-Verbindungen zu einem bestimmten internen Host explizit erlauben:

Feld	Bedeutung
Service	Dienst, der für Verbindungen zum unter **Destination** definierten Host 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* ■ *gre* ■ *esp* ■ *ah* ■ *l2tp*

Feld	Bedeutung
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 Port-Nummer des Ziel-Hosts im LAN übereinstimmen.
Destination	IP-Adresse des Hosts im LAN.

Tabelle 9-11: ***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 aktiviert.
- Bestätigen Sie mit **SAVE**.

Wenn Sie auf **X4100/200/300** NAT von einem Remote-Host z. B. mit Telnet konfigurieren, denken Sie daran, daß der Eintrag nach dem Bestätigen mit **SAVE** sofort wirksam wird!

Gehen Sie folgendermaßen vor, um an einer NAT-Schnittstelle bestimmte Verbindungen zu einem bestimmten Host im LAN freizugeben:

- Gehen Sie zu ***IP*** ➧ ***NETWORK ADDRESS TRANSLATION*** ➧ ***EDIT***.
- 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 den gewünschten Wert für **Protocol** aus.
- Geben Sie gegebenenfalls den gewünschten Wert für **Port (-1 for any)** ein.
- Geben Sie die IP-Adresse für **Destination** ein.
- Bestätigen Sie mit **SAVE**.

➤ Wiederholen Sie diese Schritte, um mehrere Freigaben für die ausgewählte NAT-Schnittstelle zu definieren.

9.2.8 Filter (Access Lists)

IP-Filter (➤➤ **Access Lists**) auf **X4100/200/300** basieren auf einem Konzept von ➤➤ **Filtern**, Regeln und sogenannten Ketten. IP-Filter reagieren auf eingehende Datenpakete. Sie können also bestimmten Daten den Zutritt zu **X4100/200/300** erlauben oder verbieten.

Filter Ein Filter beschreibt einen bestimmten Teil des IP-Datenverkehrs, basierend auf Quell- und/oder Ziel-IP-Adresse, ➤➤ **Netzmaske**, Protokoll, Quell- und/oder Ziel-Port. Wenn Sie also ein Filter definieren, teilen Sie **X4100/200/300** mit: "Achte auf diejenigen Datenpakete, auf die folgendes zutrifft: ...".

Regel Mit einer Regel teilen Sie **X4100/200/300** mit, wie der Router 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 Für die Definition von Regeln bzw. Regelketten gibt es verschiedene Ansätze:

- 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.
  - ...
  - ...
  - Weise den Rest ab.

- Kombination aus den beiden oben beschriebenen Möglichkeiten
  Es können mehrere Regelketten angelegt werden – ganz oder teilweise voneinander getrennt. Eine gemeinsame Nutzung von Filtern ist dabei möglich und sinnvoll.

Schnittstelle Schließlich können Sie für jede **X4100/200/300**-Schnittstelle individuell eine Regelkette festlegen.

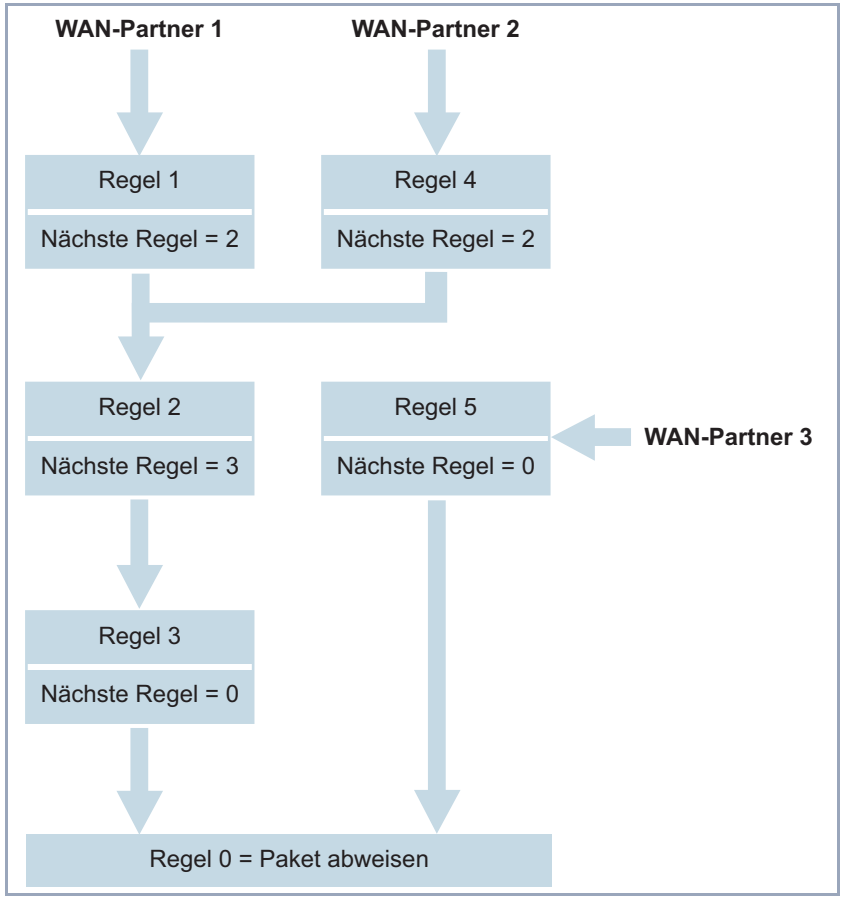


Bild 9-2: Regelketten für unterschiedliche Schnittstellen

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 nur die ersten 10 bzw. 15 Zeichen sichtbar sind.
Index	Kann hier nicht verändert werden. **X4100/200/300** vergibt hier neu definierten Filtern automatisch eine Nummer.
Protocol	Legt ein Protokoll fest. Mögliche Werte: *any, icmp, ggp, ip, tcp, egp, igp, pup, chaos, udp, hmp, xns_idp, rdp, rsvp, gre, esp, ah, tlsp, skip, kryptolan, iso-ip, igrp, ospf, ipip, ipx-in-ip, vrrp, l2tp.* *any* paßt auf jedes Protokoll, *tcp* paßt nur auf TCP-Datenpakete, usw..
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.
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 diejenigen TCP-Pakete, die beim Routing über **X4100/200/300** keine neue TCP-Verbindung öffnen würden. ■ *any:* Das Filter paßt auf alle TCP-Pakete.

Feld	Bedeutung
Source Address	Quell-IP-Adresse der Datenpakete, auf die das Filter paßt.
Source Mask	Quellnetzmaske. Durch die Kombination von **Source Address** und **Source Mask** wird ein Bereich von IP-Adressen beschrieben, auf den das Filter paßt.
Source Port	Quell-Port-Nummer bzw. Bereich von Quell-Port-Nummern, auf den das Filter paßt.
Specify Port	Bei **Source Port** bzw. **Destination Port** = *specify* bzw. *specify range:* Port-Nummern bzw. Bereich von Port-Nummern eingeben.
Destination Address	Ziel-IP-Adresse der Datenpakete, auf die das Filter paßt.
Destination Mask	Ziel-Netzmaske. Durch die Kombination von **Destination Address** und **Destination Mask** wird ein Bereich von IP-Adressen beschrieben, auf den das Filter paßt.
Destination Port	Ziel-Port-Nummer bzw. Bereich von Ziel-Port-Nummern, auf den das Filter paßt.
Type of Service (TOS)	Type of Service
TOS Mask	Bitmaske für Type of Service

Tabelle 9-12: ***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**.

Mögliche Werte	Bedeutung
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 9-13: **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 rowspan="2">Well Known Ports, d. h. fest vergeben:

priv (0..1023)</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>clients 1 (1024..4999)</td><td>server (5000..32767)</td><td>clients 2 (32768..65535)</td></tr>
</table>

Tabelle 9-14: Bereiche von Port-Nummern

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

Dienst	Protokoll	Port-Nummer
Simple Mail Transfer Protocol (SMTP)	TCP	25
Domain Name Server (➤➤ **DNS**)	TCP, UDP	53
Trivial File Transfer Protocol (➤➤ **TFTP**)	UDP	69
HTTP	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 Network Management Protocol (SNMP) (Listen Port)	UDP	161
SNMP (Trap Port)	UDP	162
Syslog Service (SYSLOG)	UDP	514
Network File System (NFS)	UDP	2049
Remote-CAPI	TCP	2662
Remote-TAPI	TCP	2663

Tabelle 9-15: 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 verwendet wird. Als Ziel-Port verwendet er die Nummer, unter der der FTP-Server den Dienst FTP anbietet, also z. B. 21. Der FTP-Server antwortet dann mit IP-Paketen, die als Quell-Port die 21 und als Ziel-Port die xyz verwenden.

Hier eine grafische Darstellung:

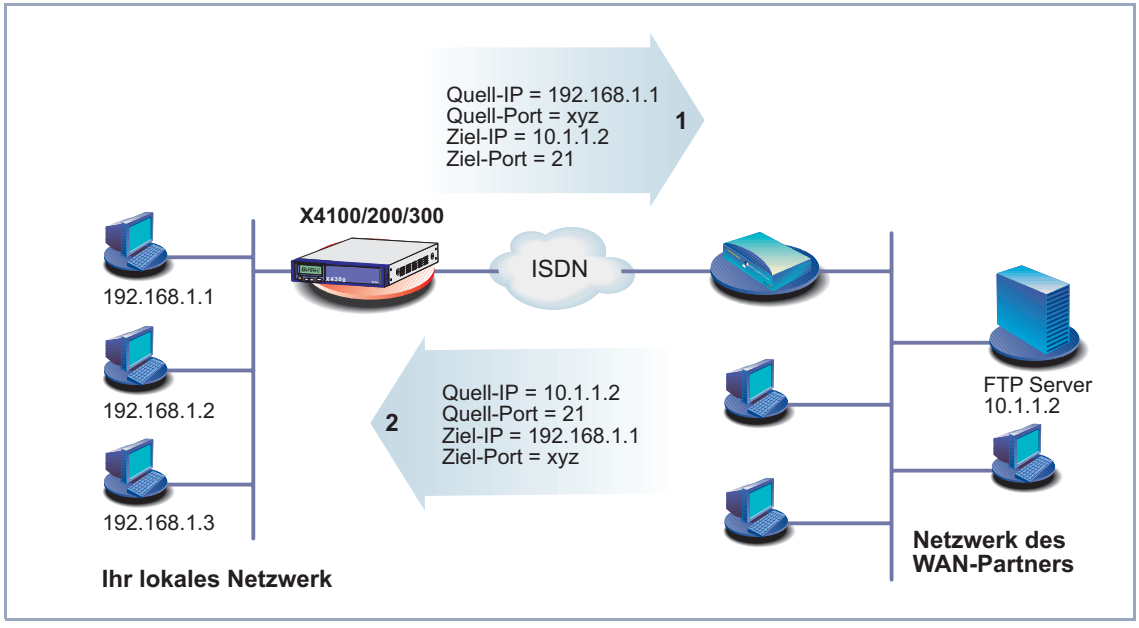


Bild 9-3: Beispiel: FTP-Verbindung

In ***IP*** ➧ ***ACCESS LISTS*** ➧ ***RULES*** definieren Sie Regeln:

Feld	Bedeutung
Index	Kann nicht verändert werden. **X4100/200/300** 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, hinter 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.

Feld	Bedeutung
Next Rule	Erscheint nur, wenn eine bestehende Regel editiert wird. Legt fest, welche Regel als nächste angewendet wird.

Tabelle 9-16: ***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 9-17: **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 diejenige Regel fest, die an erster Stelle der Kette stehen soll.

Tabelle 9-18: ***IP*** ➧ ***ACCESS LISTS*** ➧ ***RULES*** ➧ **REORG**

Wenn Sie so eine Kette neu organisieren, numeriert **X4100/200/300** nach Auswahl von **Index of Rule that gets Index 1** die verbleibenden Regeln neu:

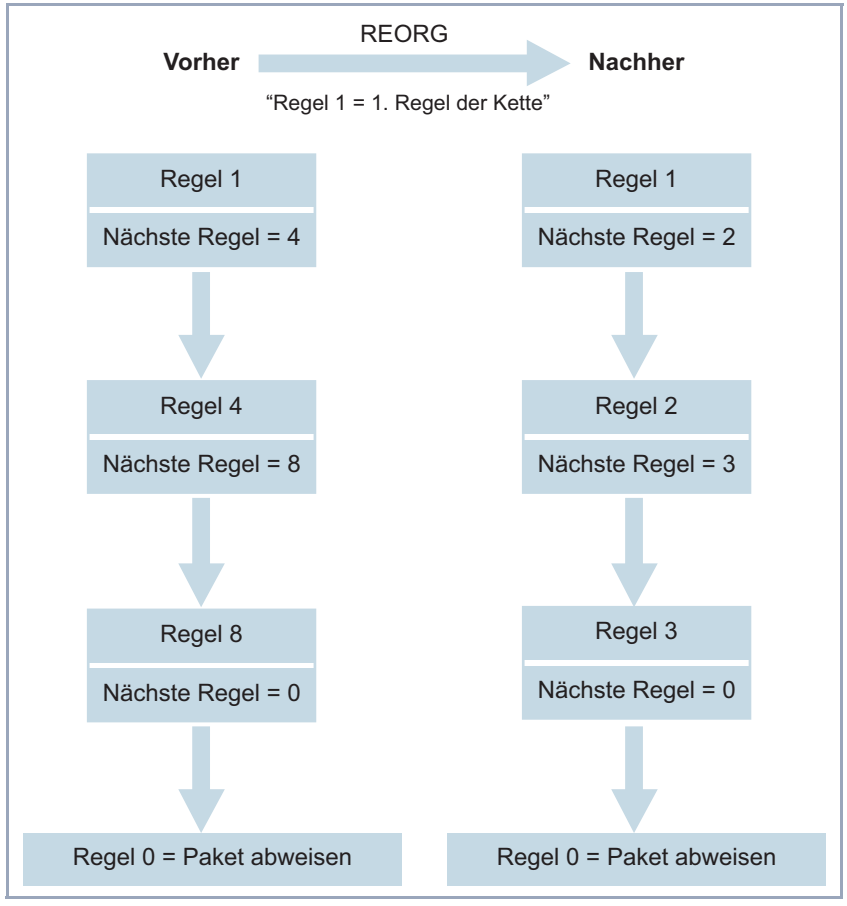


Bild 9-4: Beispiel für die Neuorganisation einer Kette

Standardmäßig wird immer die Regel mit **Index** = *1* für eine neuerstellte Schnittstelle (z. B. zu einem WAN-Partner) als erste Regel angewendet.

In ***IP*** ➧ ***ACCESS LISTS*** ➧ ***INTERFACES*** legen Sie fest, welche Schnittstelle mit welcher Regel beginnt und ob und wie der Absender eines Pakets informiert

werden soll, wenn das Paket aufgrund einer Filterverletzung von **X4100/200/300** abgewiesen wird:

Feld	Bedeutung
Interface	**X4100/200/300**-Schnittstelle
First Rule	Legt fest, welche Regel als erste für Datenpakete, die über **Interface X4100/200/300** erreichen, angewendet wird. Mit *none* legen Sie fest, daß für **Interface** keine Filter angewendet werden.
Deny Silent	Legt fest, ob der Absender eines Paketes über die Abweisung desselben aufgrund einer Filterverletzung informiert werden soll. Mögliche Werte: ■ *no*: Paket wird abgewiesen, Absender wird mit einer ICMP-Fehlermeldung darüber informiert. ■ *yes*: Paket wird abgewiesen, Absender wird nicht darüber informiert.
Reporting Method	Legt fest, ob durch die Abweisung eines Paketes aufgrund einer Filterverletzung eine Syslog-Meldung erzeugt werden soll. Mögliche Werte: ■ *none*: Keine Syslog-Meldung. ■ *info*: Eine Syslog-Meldung mit Angabe von Protokollnummer, Quell-IP-Adresse und Quell-Port-Nummer wird generiert. ■ *dump*: Eine Syslog-Meldung mit dem Inhalt der ersten 64 Bytes des abgewiesenen Pakets wird generiert.

Tabelle 9-19: ***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, kommen wirklich nur Pakete durch, die das Filter ausdrücklich erlaubt. So kann es leicht passieren, daß Ihr Zugriff auf **X4100/200/300** mit Telnet nicht mehr gestattet wird, sobald Sie die Regel eintragen und mit **SAVE** bestätigen.

- Verwenden Sie keine Filter auf dem LAN-Interface (**First Rule** = *none*), wenn Sie aus dem LAN über Telnet auf **X4100/200/300** zugreifen.

Die serielle Schnittstelle und ISDN-Login sind von den Filtereinstellungen für LAN-Interfaces unabhängig.

Filter

- Gehen Sie zu ***IP*** ➧ ***ACCESS LISTS*** ➧ ***FILTERS***.
- Fügen Sie mit **ADD** einen neuen Eintrag hinzu oder wählen Sie einen bestehenden Eintrag aus. Bestätigen mit der **Eingabetaste**, um ihn zu verändern.
- Geben Sie **Description** ein.
- Wählen Sie den gewünschten Wert für **Protocol** aus.
- Geben Sie gegebenenfalls **Source Address** ein.
- Geben Sie gegebenenfalls **Source Mask** ein.
- Wählen Sie den gewünschten Wert für **Source Port** aus.
- Geben Sie gegebenenfalls den gewünschten Wert für **Specify Port** ein.
- Geben Sie gegebenenfalls **Destination Address** ein.
- Geben Sie gegebenenfalls **Destination Mask** ein.
- Wählen Sie den gewünschten Wert für **Destination Port** aus.
- Geben Sie gegebenenfalls den gewünschten Wert für **Specify Port** ein.
- Geben Sie gegebenenfalls den gewünschten Wert für **Type of Service (TOS)** ein.
- Geben Sie gegebenenfalls den gewünschten Wert für **TOS Mask** ein.
- Bestätigen Sie mit **SAVE**.

- Wiederholen Sie diese Schritte, 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 zu 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 den gewünschten Wert für **Action** aus.
- Wählen Sie den gewünschten Wert für **Filter** aus.
- Wählen Sie **Next Rule** aus, wenn Sie eine bestehende Regel verändern.
- Bestätigen Sie mit **SAVE**.
- Wiederholen Sie diese Schritte, bis Sie alle gewünschten Regeln definiert haben.

Vergessen Sie nicht, gegebenenfalls als letzte Regel in der Kette eine Regel mit entsprechendem Filter für die Freigabe aller 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.
- Wählen Sie **Deny Silent** aus.
- Wählen Sie **Reporting Method** 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-PCs arbeiten, ist es meistens sinnvoll, ein NetBIOS-Filter zu definieren. Dieses Konfigurationsbeispiel finden Sie in Kapitel 6.1.5, Seite 115 Schritt für Schritt erläutert.

9.2.9 Lokale Filter

Der Zugang zu den lokalen UDP- bzw. TCP-Diensten auf **X4100/200/300** (Telnet, ➤➤ **CAPI**, trace, usw.) kann über ein eigenes Setup-Tool-Menü, ***IP*** ➧ ***LOCAL SERVICES ACCESS CONTROL***, geregelt werden. Für jeden Dienst können hier eine oder mehrere Einschränkungen definiert werden. Ist für einen Dienst kein Eintrag vorhanden, so gelten keine Zugriffsbeschränkungen für diesen Dienst, d. h. es kann über alle Schnittstellen und von jeder Quelladresse auf diesen Dienst zugegriffen werden, sofern dies nicht durch Einsatz von NAT (siehe Kapitel 9.2.7, Seite 334) oder globalen Filtern (siehe Kapitel 9.2.8, Seite 339) verboten wurde.

Strategie

Sobald auf **X4100/200/300** mindestens ein Eintrag für lokale Filter besteht, werden eingehende Anfragen auf die entsprechenden lokalen Dienste von **X4100/200/300** nur erlaubt, wenn eine der folgenden Bedingungen erfüllt ist:

- Die Quelladresse ist 127.0.0.1 (Loopback-Adresse).

- Es ist kein Eintrag für den entsprechenden Dienst vorhanden.
- Der eingehende Ruf wird ausdrücklich durch mindestens einen Eintrag erlaubt.

Dabei werden die vorhandenen Einträge in der Reihenfolge abgearbeitet, in der sie in der entsprechenden Tabelle in der SNMP-Shell aufgelistet sind (**localTcpAllowTable** bzw. **localUdpAllowTable**). Trifft ein Eintrag in dieser geordneten Liste nicht zu, wird der nächste Eintrag überprüft. Damit wird ermöglicht, daß Anfragen über mehrere Schnittstellen bzw. von mehreren IP-Adressen einzeln auf einen bestimmten Dienst zugelassen werden können.

Wurde auch nach Überprüfung des letzten Eintrags in der Liste kein passender Eintrag für eine Anfrage gefunden, gibt es zwei Alternativen:

- Die Anfrage wird an den entsprechenden Dienst weitergeleitet, wenn kein Eintrag in der Liste sich auf diesen Dienst bezieht.
- Die Anfrage wird abgelehnt, wenn ein oder mehrere Einträge in der Liste für diesen Dienst existieren, aber keiner auf die Anfrage zutrifft.

Lokale Filter sind also ein zusätzliches Instrument, das aber anders zu handhaben ist als die globalen Filter und zudem die Performanz beim normalen Routing nicht beeinträchtigt.

Die Konfiguration erfolgt in ***IP*** ➧ ***LOCAL SERVICES ACCESS CONTROL*** ➧ **ADD**:

Feld	Bedeutung
Service	Definiert den lokalen Dienst auf **X4100/200/300**, zu dem der Zugang u. a. mit diesem Eintrag geregelt werden soll. Mögliche Werte: ■ *snmp(udp)* ■ *rip (udp)* ■ *bootps(udp)* ■ *dns(udp)* ■ *telnet(tcp)* ■ *trace(tcp)* ■ *snmp(tcp)* ■ *capi(tcp)* ■ *tapi(tcp)* ■ *rfc1086(tcp)* ■ *http(tcp)* ■ *nbns(udp)* ■ *statmon(udp)*
Verify IP Address	Definiert, ob bei einem eingehenden Ruf auf den unter **Service** festgelegten Dienst die Quell-IP-Adresse überprüft werden soll. Mögliche Werte: ■ *verify* ■ *don't verify*

Feld	Bedeutung
IP Address	(nur bei **Verify IP Address** = *verify*) Definiert eine IP-Adresse bzw. Netzwerkadresse (zusammen mit **Mask**), von der eingehende Anfragen auf den unter **Service** festgelegten Dienst erlaubt werden. Hat eine Anfrage eine andere Quelladresse, wird zum nächsten Eintrag übergegangen.
Mask	(nur bei **Verify IP Address** = *verify*) Definiert eine Netzmaske. Zusammen mit **IP Address** wird damit eine Netzwerkadresse definiert, von der eingehende Anfragen auf den unter **Service** festgelegten Dienst erlaubt werden. Hat eine Anfrage eine andere Quelladresse, wird zum nächsten Eintrag übergegangen. Ist der Wert von **Mask** *0.0.0.0* oder *255.255.255.255*, handelt es sich um einen Host-Eintrag, d. h. die IP-Adresse muß exakt passen.
Verify Interface	Definiert, ob bei einem eingehenden Ruf auf den unter **Service** festgelegten Dienst überprüft werden soll, über welche **X4100/200/300**-Schnittstelle der Ruf eingeht. Mögliche Werte: ■ *verify* ■ *don't verify*

Feld	Bedeutung
Interface	(nur bei **Verify Interface** = *verify*) Definiert eine Schnittstelle von **X4100/200/300**. Erreicht **X4100/200/300** ein eingehender Ruf auf den unter **Service** festgelegten Dienst über diese Schnittstelle, wird die Verbindung erlaubt. Überquert der eingehende Ruf eine andere Schnittstelle, wird zum nächsten Eintrag übergegangen.

Tabelle 9-20: ***IP*** ➧ ***LOCAL SERVICES ACCESS CONTROL*** ➧ **ADD**

Gehen Sie folgendermaßen vor, um den Zugang zu einem lokalen Dienst einzuschränken:

Wenn mit einem Eintrag sowohl eine Adresse als auch eine Schnittstelle zur Überprüfung festgelegt wird, müssen bei einem eingehenden Ruf beide Kriterien erfüllt sein, damit **X4100/200/300** den Ruf annimmt.

- Gehen Sie zu ***IP*** ➧ ***LOCAL SERVICES ACCESS CONTROL***.
  Hier sind alle bisher vorgenommenen Einträge aufgelistet.
- Betätigen Sie **ADD**, um einen neuen Eintrag hinzuzufügen.
- Wählen Sie den gewünschten Wert für **Service** aus.
- Wählen Sie **Verify IP Address** aus, z. B. ***verify***.
- Geben Sie gegebenenfalls die gewünschte **IP Address** ein.
- Geben Sie gegebenenfalls die gewünschte **Mask** ein.
- Wählen Sie **Verify Interface** aus, z. B. ***verify***.
- Wählen Sie gegebenenfalls den gewünschten Wert für **Interface** aus.
- Bestätigen Sie mit **SAVE**.
  Der Eintrag wird aufgelistet.

9.2.10 Backroute Verification

Hinter diesem Begriff versteckt sich eine einfache, aber sehr leistungsfähige Funktion von **X4100/200/300**. 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 Sie 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**.
  Backroute Verification ist aktiviert.

9.2.11 TAF-Agent

Personenbezogene Authentisierung

Die Funktion Token Authentication Firewall (TAF) ermöglicht eine personenbezogene Authentisierung von IP-Verbindungspartnern. BinTecs 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 **X4100/200/300** können Sie diese Funktion freischalten (mit Zusatzlizenz) und den Router als TAF-Agent einrichten. Die genaue Darstellung der Funktionsweise und die erforderlichen Konfigurationsschritte finden Sie in **BRICKware for Windows** und in der **Software Reference**.

9.2.12 Extended IP-Routing (XIPR)

Ergänzend zu der normalen Routing-Tabelle kann **X4100/200/300** auch Routing-Entscheidungen aufgrund einer zusätzlichen Tabelle, der Extended-Routing-Tabelle, treffen (Erweitertes IP-Routing). Dabei kann **X4100/200/300** neben der Quell- und Zieladresse u. a. auch das Protokoll, Quell- und Ziel-Port, Art des Dienstes (Type of Service, TOS) und den Status der Ziel-Schnittstelle in die Entscheidung mit einbeziehen. Wenn Einträge in der Extended-Routing-Tabelle stehen, werden diese gegenüber den Einträgen in der normalen Routing-Tabelle bevorzugt behandelt.

Beispiel 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**).

Konfiguration Die Konfiguration erfolgt im Setup-Tool-Menü ***IP*** ➧ ***ROUTING*** ➧ **ADDEXT**:

```
X4x00 Setup Tool                          BinTec Access Networks GmbH
[IP][ROUTING][ADD]: IP Routing - Extended Route                MyRouter

Route Type              Network route
Network                 WAN without transit network

Destination IP-Address
Netmask
Partner / Interface     BigBoss          Mode    always

Netmask

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


                    SAVE                CANCEL

Use <Space> to select
```

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), siehe Tabelle 9-22, Seite 359.
Destination IP-Address	IP-Adresse des Ziel-Hosts oder -LANs.
Netmask	Netzmaske von **Destination IP-Address**.
Partner / Interface	WAN-Partner (nur möglich bei **Network** = *WAN without transit network*)
Mode	Definiert, wann das unter **Partner / Interface** gewählte Interface benutzt werden soll.
Metric	Je niedriger der Wert, desto höhere Priorität besitzt die Route (Wertebereich *0...15*).
Source Interface	Schnittstelle, über die die Datenpakete die **X4100/200/300** erreichen.
Source IP-Address	Quell-IP-Adresse des Quell-Hosts bzw. -LANs.
Source Mask	Quellnetzmaske.
Type of Service (TOS)	Mögliche Werte: *0..255* als Bitfolge.
TOS Mask	Bitmaske für **Type of Service**.
Protocol	Legt ein Protokoll fest. Mögliche Werte: *tcp, egp, pup, udp, hmp, xns, rdp, rsvp, gre, esp, ah, igrp, ospf, l2tp*, *dont ver*, *icmp, ggp.*
Source Port	Quell-Port-Nummer bzw. Bereich von Quell-Port-Nummern (siehe Tabelle 9-24, Seite 360).

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

Tabelle 9-21: ***IP*** ➧ ***ROUTING*** ➧ ***ADDEXT***

Das Feld **Network** enthält folgende Auswahlmöglichkeiten:

Mögliche Werte	Bedeutung
LAN	Route zu einem Ziel-Host oder -LAN, das über **X4100/200/300**s LAN-Anschluß zu erreichen ist.
WAN without transit network	Route zu einem Ziel-Host oder -LAN, welche über einen WAN-Partner ohne Berücksichtigung eines evtl. vorhandenen Transitnetzwerks zu erreichen sind.
WAN with transit network	Route zu einem Ziel-Host oder -LAN, welche über einen WAN-Partner nur über ein Transitnetzwerk zu erreichen sind.
Refuse	**X4100/200/300** verwirft Datenpakete, die diese Route benutzen, und übermittelt dem Absender eine Meldung, daß das Ziel des Paketes unerreichbar ist.
Ignore	**X4100/200/300** verwirft Datenpakete, die diese Route benutzen, ohne eine Statusmeldung zu senden.

Tabelle 9-22: **Network**

Das Feld **Mode** enthält folgende Auswahlmöglichkeiten:

Mögliche Werte	Bedeutung
always	Route immer benutzen.

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

Tabelle 9-23: **Mode**

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.
specify range	Ermöglicht Eingabe eines Bereiches von Port-Nummern.
priv (0..1023)	Port-Nummern: 0 ... 1023.
server (5000..32767)	Port-Nummern: 5000 ... 32767.
clients 1 (1024..4999)	Port-Nummern: 1024 ... 4999.
clients 2 (32768..65535)	Port-Nummern: 32768 ... 65535.
unpriv (1024..65535)	Port-Nummern: 1024 ... 65535.

Tabelle 9-24: **Source Port** bzw. **Destination Port**

Konfiguration

Gehen Sie folgendermaßen vor, um erweitertes IP-Routing zu konfigurieren:

➤ Gehen Sie zu ***IP*** ➧ ***ROUTING*** ➧ **ADDEXT**.

➤ Wählen Sie eine **Route Type** aus.

- Wählen Sie das gewünschte **Network** aus.
- Tragen Sie die gewünschte **Destination IP-Address** ein.
- Tragen Sie die gewünschte **Netmask** ein.
- Wählen Sie das gewünschte **Partner / Interface** aus.
- Wählen Sie den gewünschten **Mode** aus.
- Tragen Sie die gewünschte **Metric** ein.
- Wählen Sie das gewünschte **Source Interface** aus.
- Geben Sie die gewünschte **Source IP-Address** ein.
- Geben Sie die gewünschte **Source Mask** ein.
- Wählen Sie **Type of Service** aus.
- Tragen Sie die **TOS Mask** ein.
- Wählen Sie das gewünschte **Protocol** aus.
- Wählen Sie den gewünschten **Source Port** aus.
- Wählen Sie den gewünschten **Destination Port** aus.
- Spezifizieren Sie gegebenenfalls **Source Port**.
- Spezifizieren Sie gegebenenfalls **Destination Port**.
- Bestätigen Sie mit **SAVE**.

  Erweitertes IP-Routing ist für die eingetragenen Schnittstellen konfiguriert.

Eine ausführliche Beschreibung (einschließlich der Konfiguration anhand der MIB-Variablen) finden Sie in der **Software Reference**.

9.3 Abhörsicherung

Für PPP-Verbindungen auf sicherheitskritischen Verbindungen können Sie einen Verschlüsselungsmechanismus einsetzen, wenn beide Verbindungspartner diesen unterstützen. Folgende Funktionen sind möglich:

- Verschlüsselung (Kapitel 9.3.1, Seite 362)
- VPN (mit Zusatzlizenz, Kapitel 9.3.2, Seite 366)
- IPSec (mit Zusatzlizenz, Kapitel 9.3.3, Seite 366)
- Festverbindungen (leased line, Kapitel 9.3.4, Seite 367)

9.3.1 Verschlüsselung

X4100/200/300 unterstützt Verschlüsselung von PPP-Verbindungen mit WAN-Partnern.

Dabei werden die Verfahren ➤➤ **MPPE** (Microsoft Point to Point ➤➤ **Encryption**) Version 1 und 2, DES und Blowfish eingesetzt. DES und Blowfish sind als BinTec-proprietäre Lösungen realisiert.

MPPE V2

Das Verschlüsselungsprotokoll MPPE Version 2, Nachfolger von MPPE, wurde von Microsoft entwickelt und verwendet ebenso einen 40-Bit- oder 56-Bit-Schlüssel. Diese werden bei der Authentisierung generiert.

Wenn auf **X4100/200/300** eine höhere Schlüssellänge eingestellt ist als auf einem einwählenden Dial-in-Client, kommt die Verbindung nicht zustande.

Wenn bei einem Verbindungspartner MPPE V1 als Verschlüsselungsprotokoll eingestellt ist, wird beim Verbindungsaufbau auch MPPE V2 akzeptiert, falls die eingestellte Schlüssellänge übereinstimmt.

DES und Blowfish

Bei Verwendung dieser proprietären Verschlüsselungsalgorithmen kann **X4100/200/300** entweder einen Schlüssel automatisch generieren oder Sie definieren in Abstimmung mit dem Verbindungspartner statisch einen individuellen Schlüssel.

Die Verschlüsselungsalgorithmen DES und Blowfish werden nur unterstützt, wenn auf **X4100/200/300** eine Lizenz für VPN eingetragen ist.

Die Konfiguration erfolgt in den Menüs:

- ***WAN PARTNER*** ➧ ***EDIT***
- ***WAN PARTNER*** ➧ **EDIT** ➧ ***ADVANCED SETTINGS*** ➧ ***EXTENDED INTERFACE SETTINGS (OPTIONAL)***

Folgendes Feld in ***WAN PARTNER*** ➧ ***EDIT*** ist für diesen Konfigurationsschritt relevant:

Feld	Bedeutung
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:* MPPE Version 1 mit 40-Bit-Schlüssel ■ *MPPE 56:* MPPE Version 1 mit 56-Bit-Schlüssel ■ *MPPE 128:* MPPE Version 1 mit 128-Bit-Schlüssel ■ *MPPE V2 40:* MPPE Version 2 mit 40-Bit-Schlüssel ■ *MPPE V2 56:* MPPE Version 2 mit 56-Bit-Schlüssel ■ *MPPE V2 128:* MPPE Version 2 mit 128-Bit-Schlüssel ■ *DES 56*: DES mit 56-Bit-Schlüssel ■ *Blowfish 56*: Blowfish mit 56-Bit-Schlüssel ■ *none:* keine Verschlüsselung Diese Werte sind nur verfügbar, wenn unter **Encapsulation** *PPP*, *Async PPP over X.75*, *Async PPP over X.75/T.70/BTX* oder *X.25_PPP* ausgewählt wurde.

Tabelle 9-25: ***WAN PARTNER*** ➧ ***EDIT***

Bei Verwendung von DES oder Blowfish kann der Schlüssel mit der Authentisierung automatisch generiert oder statisch definiert werden. Dafür sind im

Menü ***WAN PARTNER*** ➧ **EDIT** ➧ ***ADVANCED SETTINGS*** ➧ ***EXTENDED INTERFACE SETTINGS (OPTIONAL)*** folgende Felder relevant:

Feld	Bedeutung
Encryption Key Negotiation	Definiert, ob ein Schlüssel für die Verbindung zum WAN-Partner automatisch generiert oder statisch definiert wird. Mögliche Werte: ■ *authentication* (Standardwert): Schlüssel wird von **X4100/200/300** automatisch generiert. ■ *static*: Schlüssel wird statisch definiert und muß unter **Encryption Key (TX)** bzw. **Encryption Key (RX)** eingetragen werden.
Encryption Key (TX)	(nur bei **Encryption Key Negotiation** = *static*) Schlüssel (im hexadezimalen Format) zur Verschlüsselung ausgehender Daten (muß mit dem Eintrag unter **Encryption Key (RX)** beim Verbindungspartner übereinstimmen).
Encryption Key (RX)	(nur bei **Encryption Key Negotiation** = *static*) Schlüssel (im hexadezimalen Format) zur Verschlüsselung eingehender Daten (muß mit dem Eintrag unter **Encryption Key (TX)** beim Verbindungspartner übereinstimmen).

Tabelle 9-26: ***WAN PARTNER*** ➧ **ADD** ➧ ***ADVANCED SETTINGS*** ➧ ***EXTENDED INTERFACE SETTINGS (OPTIONAL)***

ToDo Gehen Sie folgendermaßen vor, um Daten mit einem WAN-Partner in verschlüsselter Form auszutauschen:

➤ Gehen Sie zu ***WAN PARTNER***.

➤ Wählen Sie einen WAN-Partner aus und bestätigen Sie mit der **Eingabetaste**, um PPP-Verbindungen mit diesem Partner zu verschlüsseln.

- Wählen Sie **Encryption** aus, z. B. ***DES 56***.
- Gehen Sie zu ***WAN PARTNER*** ➧ **EDIT** ➧ ***ADVANCED SETTINGS*** ➧ ***EXTENDED INTERFACE SETTINGS (OPTIONAL)***.
- Wählen Sie **Encryption Key Negotiation** aus, z. B. ***static*** (wenn Sie den Schlüssel selbst definieren möchten).
- Geben Sie gegebenenfalls **Encryption Key (TX)** ein, z. B. ***1A35EFC17B56***.
- Geben Sie gegebenenfalls **Encryption Key (RX)** ein, z. B. ***89A1288CD131***.
- Bestätigen Sie mit **SAVE**.
- Bestätigen Sie mit **OK**.
- Bestätigen Sie mit **SAVE**.

  Die PPP-Verbindung mit dem gewählten VPN-Partner wird verschlüsselt.

9.3.2 VPN (mit Zusatzlizenz)

Mit Hilfe von PPTP (Point to Point Tunneling Protocol) kann **X4100/200/300** ein VPN (Virtual Private Network) herstellen. Dies dient der sicheren 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 **Software Reference**.

9.3.3 IPSec (mit Zusatzlizenz)

Der Sicherheitsstandard IPSec (Internet Protocol Security) ermöglicht Ihnen, IP-basierte Daten sicher über öffentliche Netze (z. B. das Internet) auszutauschen.

Immer mehr Unternehmen wickeln immer mehr Datenkommunikation über das Internet ab. Um dennoch sicher zu sein, daß ihre Daten vertraulich bleiben und nicht von Dritten eingesehen oder mißbraucht werden, setzen diese Unternehmen zusehens Verschlüsselungstechnologien ein. Es wurden eine ganze Reihe zum Teil standardisierter Verfahren entwickelt, welche die technischen Grundlagen für verschiedene VPN-Lösungen darstellen. In den letzten Jahren haben sich die Verfahren PPTP (Point-to-Point Tunneling Protocol) und IPSec (IP Security) als vielversprechende Lösungen durchgesetzt. Der **X4100/200/300** unterstützt beide Verfahren.

Während PPTP die Daten in einem Tunnel auf Schicht 2 (OSI Modell) überträgt, arbeitet IPSec auf Schicht 3. Die Daten werden dabei mit einer Schlüssellänge von bis zu 168 Bit verschlüsselt. Darüber hinaus bietet IPSec Verfahren zur Authentisierung und Verwaltung von Schlüsseln. Da IPSec auf der Schicht 3 arbeitet, ist es für den Benutzer vollständig transparent. Dies bedeutet, daß die zu sendenden Daten in jedem Fall stark verschlüsselt werden, ohne daß der Benutzer aktiv werden muß. Die Verschlüsselung und die Aushandlung der unterschiedlichen Schlüssel werden entweder vom Router oder bei Einzelarbeitsplätzen von einem IPSec-Client übernommen, der auf dem Arbeitsplatzrechner installiert wurde. BinTec bietet einen solchen Client im Zusammenhang mit der BinTec IPSec-Lösung an.

Sollten Sie eine IPSec-Lösung mit dem **X4100/200/300** realisieren wollen, so benötigen Sie hierzu eine IPSec-Zusatzlizenz. Diese erhalten Sie bei Ihrem Fachhändler.

Detaillierte Informationen und Konfigurationshinweise finden Sie im **IPSec Reference Manual**, das Sie zusammen mit Ihrer IPSec-Lizenz erhalten.

9.3.4 Festverbindungen (leased lines)

Sie können die ISDN-BRI- und ISDN-PRI-Schnittstellen von **X4100/200/300** nicht nur für Wählverbindungen, sondern auch für Festverbindungen nutzen.

Konfigurationshinweise finden Sie in Kapitel 6.2, Seite 121, und Kapitel 6.3, Seite 147.

9.4 Besonderheiten

Folgende Besonderheiten unterstützen die Sicherheit Ihres Netzwerks:

- Startup-Verhalten (Kapitel 9.4.1, Seite 368)
- Auto-Logout (Kapitel 9.4.2, Seite 368)
- Vorbeugung gegen Denial-of-Service-Attacken (Kapitel 9.4.3, Seite 368)

9.4.1 Startup-Verhalten

X4100/200/300 nimmt die Routing-Tätigkeiten erst auf, wenn die komplette Konfiguration, insbesondere auch die definierten Filter, geladen ist. 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.

9.4.2 Auto-Logout

Verbindungen zu **X4100/200/300** über Telnet, ➤➤ **ISDN-Login** 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 13.1, Seite 418).

9.4.3 Vorbeugung gegen Denial-of-Service-Attacken

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.

Einige DoS-Attacken auf den Router selbst werden bereits durch die interne Codierung unterbunden.

Es existiert z. B. an allen **X4100/200/300**-Schnittstellen, für die Sie Network Address Translation (NAT) aktivieren, ein Schutz für die angeschlossenen Rechner gegen einige DoS-Attacken mit fragmentierten Paketen. Die Paketfragmente werden 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 9.2.10, Seite 356).

DoS-Angriffe, die auf Systemstörung durch Überlaufen von Log-Dateien (Syslog-Messages) spekulieren, können Sie durch geeignete Plazierung und Größenlimitierung dieser Dateien begegnen.

9.5 Checkliste

Die nachfolgende Liste gibt die wichtigsten sicherheitskritischen Punkte an, die Sie bei der Konfiguration von **X4100/200/300** beachten sollten:

- Haben Sie alle vier Paßwörter für den Systemzugang (`admin`, `read`, `write`) verändert? Siehe Kapitel 4.2, Seite 62.
- Werden die Aktivitäten von **X4100/200/300** auf mindestens einem externen Rechner ausreichend genau protokolliert und überprüfen Sie die Syslog-Messages regelmäßig? Siehe Kapitel 9.1.1, Seite 312.
- Haben Sie den Zugriff auf die lokalen Dienste und Ressourcen eingeschränkt auf bekannte Rechner oder Netze? Insbesondere die Zugänge per CAPI, SNMP, 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 ggf. für die Verbindung zum Internet Service Provider (ISP) Network Address Translation (NAT) aktiviert? Siehe Kapitel 9.2.7, Seite 334.
- Haben Sie an kritischen Schnittstellen den IP-Datenverkehr ggf. mit Hilfe von Filtern eingeschränkt und IP-Address-Spoofing verhindert? Dabei sollten Sie besonders die Schnittstellen beachten, die Sie nicht durch NAT abgesichert haben! Siehe Kapitel 9.2.8, Seite 339.
- Haben Sie ggf. den Zugang über ISDN-Login für Fernwartung gesperrt? Haben Sie einen geeigneten Eintrag unter ***CM1BRI, ISDN S0*** ➧ ***INCOMING CALL ANSWERING*** gemacht? Siehe "Incoming Call Answering", Seite 125.

Als zusätzliche Punkte sollten Sie beachten:

- Verwenden Sie für PPP-Verbindungen Callback nach dem Microsoft-Verfahren? Beachten Sie bitte die Hinweise in Kapitel 9.2.4, Seite 331.
- Setzen Sie auf sicherheitskritischen Verbindungen ein Verschlüsselungsprotokoll zur Abhörsicherung ein? Siehe Kapitel 9.3.1, Seite 362.

- 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 7.2.9, Seite 220.
- 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 BinTecs User-Konzept (Kapitel 6.3, Seite 147)?
- Sind eventuell zusätzlich angelegte Benutzer-Accounts unproblematisch?
- Haben Sie das Abhören von Verbindungen auf dem Ethernet durch eine geeignete LAN-Infrastruktur verhindert?

10 Konfigurationsmanagement

In diesem Kapitel finden Sie Hinweise zum Verwalten Ihrer Konfigurationsdateien und zum Updaten der Software von **X4100/200/300**. Es umfaßt folgende Bereiche:

- Verwalten der Konfigurationsdateien (Kapitel 10.1, Seite 374)
  - Wo sind die Konfigurationsdateien?
  - Was ist Flash und Memory?
  - Wie kann ich mit Konfigurationsdateien umgehen?
- Software-Update durchführen (Kapitel 10.2, Seite 382)
  - Wie bleibe ich immer auf dem neuesten Stand?
  - Wie lade ich ein neues Boot-Image?

10.1 Konfigurationsdateien verwalten

Flash **X4100/200/300** liest seine Konfigurationsinformationen aus Konfigurationsdateien. Diese Konfigurationsdateien sind gespeichert im Flash EEPROM (electronically erasable programmable read-only memory) von **X4100/200/300**. Im Flash-Speicher können einige verschiedene Konfigurationsdateien gespeichert werden. Auch wenn **X4100/200/300** 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 **X4100/200/300** einstellen. Der Inhalt des Memorys geht verloren, wenn **X4100/200/300** ausgeschaltet wird. Wenn Sie Ihre Konfiguration ändern und diese Änderungen auch beim nächsten Start von **X4100/200/300** beibehalten wollen, müssen Sie die geänderte Konfiguration vor dem Ausschalten im Flash speichern: **Exit** ➧ **Save as boot configuration and exit** (siehe Kapitel 6.4, Seite 176). Diese Datei wird damit als Boot-Konfigurationsdatei mit dem Namen "boot" im Flash gespeichert. Beim Starten von **X4100/200/300** wird dann genau diese Datei, also die Konfigurationsdatei mit dem Namen "boot", ins 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 **X4100/200/300** 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 **X4100/200/300** auf Ihrem lokalen Rechner abspeichern.

Die mit dem TFTP-Server der DIME Tools zu transferierenden Dateien dürfen maximal aus acht Zeichen bestehen (plus maximal drei Zeichen als Anhang), z. B. ***b5104.x4a***.

Unix Unter Unix ist ein TFTP-Server Teil des Systems, beachten Sie bitte die Hinweise in der **Software Reference**.

Mit dem Setup Tools können Sie die verschiedenen Aktionen ausführen:

➤ Gehen Sie in das Menü ***CONFIGURATION MANAGEMENT***.

Folgendes Menü öffnet sich:

```
X4x00 Setup Tool                          BinTec Access Networks GmbH
[CONFIG]: Configuration Management                          MyRouter

    Operation                   get  (TFTP --> FLASH)

    TFTP Server IP Address      192.168.1.1
    TFTP File Name              b5104.x4a

    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 Host-Name (falls der Host-Name 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 **X4100/200/300**-Start).
State of last operation	Status der letzten Aktion.

Tabelle 10-1: ***CONFIGURATION MANAGEMENT***

Das Feld **Operation** enthält folgende Auswahlmöglichkeiten:

Mögliche Werte	Bedeutung
save (MEMORY --> FLASH)	Alle aktuellen Einstellungen vom 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 **X4100/200/300** 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	**X4100/200/300** neu starten. Einstellungen im Memory werden durch Einstellungen von "boot" aus Flash ersetzt.

Tabelle 10-2: **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-Messages).

Tabelle 10-3: **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 **X4100/200/300**s Boot-Datei gelöscht, **X4100/200/300** 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 und 98:

- 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 und 2000:

- 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** die richtige IP-Adresse angegeben?
- Bei Verwendung älterer Versionen der **BRICKware for Windows**: Besteht der Name der Konfigurationsdatei aus höchstens acht Zeichen und die Extension aus höchstens drei Zeichen (bei Verwendung der **DIME Tools**)?
- Unterstützt der Host TFTP (haben Sie vor Ausführen der Aktion den TFTP-Server der **DIME Tools** gestartet)?
- Liegt die Quelldatei im konfigurierten Verzeichnis des TFTP-Pfades der **DIME Tools** (Bei **Operation** = *get*)? Beachten Sie **BRICKware for Windows**, um den TFTP-Pfad zu verändern.

Sind bei obigen Punkten keine Fehler zu finden, 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.

➤ Verlassen Sie ***CONFIGURATION MANAGEMENT*** mit **EXIT**.

Beispiel Sie haben die Konfigurationsdatei brick.cf erstellt. Sie haben die Datei nicht über die serielle Schnittstelle auf **X4100/200/300** 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 **X4100/200/300** 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 MANGAGEMENT***.

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**.

  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 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 **X4100/200/300** gespeichert.

Gehen Sie anschließend folgendermaßen vor, um die Einstellungen von brick.cf sofort auf **X4100/200/300** 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**.

  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 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 **X4100/200/300** 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.

10.2 Software-Update durchführen

Da BinTec Access Networks GmbH die Software für alle Produkte ständig weiterentwickelt und Sie sicher die neuen Funktionen von **X4100/200/300** nutzen wollen, erfahren Sie hier, wie Sie ein Software-Update durchführen können.

www.bintec.de

Wenn Sie ein Software-Update durchführen, spielen Sie auf **X4100/200/300** ein neues Software-Image (Boot-Image) ein. Jedes Boot-Image beinhaltet neue Funktionen, bessere Performanz und bei Bedarf Bugfixes der vorhergehenden Version. Die aktuellen von BinTec Access Networks GmbH kostenlos zur Verfügung gestellten Software-Images finden Sie im World Wide Web unter www.bintec.de. Hier finden Sie auch aktuelle produktspezifische Dokumentation (**Release Notes**, **Benutzerhandbücher**, **Kurzanleitungen**) und produktübergreifende Dokumentation (**Software Reference**, **BRICKware for Windows**).

Wenn Sie ein Software-Update durchführen, beachten Sie unbedingt die dazugehörige **Release Notes**. 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 3.6, Seite 52.

Achtung!

In seltenen Fällen ist zusätzlich ein Update von Modullogik, BOOTmonitor und/oder Firmware Logic empfohlen. Falls dies bei einem neuen Release nötig sein sollte, ist dies ausdrücklich in den entsprechenden **Release Notes** vermerkt. Die Vorgehensweise und Empfehlung finden Sie in den **Release Notes** "BOOTmonitor and Firmware Logic Update" unter www.bintec.de (Abschnitt "Download").
Die Folge von fehlerhaft durchgeführten Update-Vorgängen (z. B. Stromausfall während des Updates) könnte sein, daß **X4100/200/300** nicht mehr bootet!

- Updaten Sie Modullogik, BOOTmonitor oder Firmware Logic nur, wenn BinTec Access Networks GmbH eine explizite Empfehlung dazu ausspricht!

ToDo Gehen Sie folgendermaßen vor, um ein Software-Update (Boot-Image) durchzuführen:

Schalten Sie **X4100/200/300** 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 öffnet sich.

- Klicken Sie auf "Lösungen und Produkte" und anschließend auf "Download".

  Dort finden Sie die aktuelle Software und Dokumentation für BinTec-Produkte.

- Klicken Sie auf "X4000".

  Dort finden Sie die aktuelle Software und Dokumentation für **X4100/200/300**.

- Klicken Sie mit der rechten Maustaste auf das aktuelle Boot-Image, z. B. **Boot-Image Rel. 5.1 Rev.4**.

- 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). Den Namen können Sie 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 Kapitel 4.5.2, Seite 80). Aktivieren Sie den TFTP-Server.
  Unix-Rechner: Beachten Sie die Hinweise in der **Software Reference**.
- Loggen Sie sich auf **X4100/200/300** 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.

  Die Datei `<Dateiname>` wird zunächst in den Arbeitsspeicher von **X4100/200/300** 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.

Achtung!

Die Unterbrechung des "incremental update" hat zur Folge, daß **X4100/200/300** nicht mehr booten kann und die Konfiguration zerstört ist!

- Stellen Sie sicher, daß das "incremental update" nicht unterbrochen wird!

X4100/200/300 benötigt einen zusammenhängenden Block an freiem Arbeitsspeicher, der etwas größer als das neue Software-Image ist. Wenn auf **X4100/200/300** nicht genügend Arbeitsspeicher zu Verfügung steht, bietet **X4100/200/300** 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 und 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**.

  X4100/200/300 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**.

  X4100/200/300 startet mit dem neuen Boot-Image. Die vorhandene Konfiguration wird überschrieben.

11 Troubleshooting

Tips Wenn Sie Probleme mit **X4100/200/300** haben, helfen Ihnen die folgenden Tips häufig schon weiter:

- Loggen Sie sich auf **X4100/200/300** 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 **X4100/200/300** erzeugten Syslog-Messages (siehe Kapitel 9.1.1, Seite 312). 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 (Kapitel 11.1, Seite 388)
- Typische Fehlersituationen (Kapitel 11.2, Seite 391)

11.1 Hilfsmittel zum Troubleshooting

Hier finden Sie Hilfsmittel, um die Ursache Ihres Problems einzugrenzen:

- Eingabetasten und Display zur Bedienung des Man Machine Interface (MMI)
- Lokale SNMP-Shell-Kommandos
- Externe Hilfsmittel

11.1.1 Man Machine Interface (MMI)

Mit dem MMI können Sie sich über das Display einige Informationen über den Status von **X4100/200/300** (Grundgerät und Erweiterungskarte) anzeigen lassen, ohne sich auf dem Gerät einloggen zu müssen. Z. B. sind auf diesem Weg die Version des aktuellen Software-Releases oder der aktuelle Betriebszustand der Schnittstellen schnell zu erreichen.

Das MMI ist einfach zu bedienen und Sie können den Display-Meldungen intuitiv folgen. Eine detaillierte Beschreibung finden Sie in Kapitel 5, Seite 83.

11.1.2 Lokale SNMP-Shell-Kommandos

Diese Kommandos geben Sie direkt in die SNMP-Shell von **X4100/200/300** ein:

debug

Mit dem Kommando `debug` können Sie die Fehlersuche für eines oder mehrere Subsysteme von **X4100/200/300** betreiben. Eine genaue Erläuterung der Syntax und der Optionen finden Sie in Kapitel 13.1, Seite 418.

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 10, Seite 373).

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 13.1, Seite 418.

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 13.1, Seite 418.

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 **X4100/200/300**s MAC-Adresse über das LAN zum Host mit der MAC-Adresse 0:a0:f9:d:5:a verschickt werden.

11.1.3 Externe Hilfsmittel

Mit den folgenden Hilfsprogrammen können Sie von einem Windows-PC oder einem Unix-Rechner aus Verbindungen mit **X4100/200/300** analysieren.

DIME Tracer (Windows)

Der DIME Tracer ermöglicht, **X4100/200/300**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 **X4100/200/300**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 13.2, Seite 425.

11.2 Typische Fehlersituationen und Vorgehensweise

Im folgenden finden Sie eine Zusammenstellung typischer Fehlersituationen und Hinweise zu Diagnose und "Heilung". Versuchen Sie, das auftretende Problem einzugrenzen. Das Kapitel ist in zwei Kategorien aufgeteilt:

- System-Fehler (Kapitel 11.2.1, Seite 391)
- ISDN-Verbindungen (Kapitel 11.2.2, Seite 392)

11.2.1 System-Fehler

Ich habe mein Paßwort vergessen.

Sie müssen **X4100/200/300** in den unkonfigurierten Anfangszustand (Auslieferungszustand) zurückversetzen:

- Verbinden Sie Ihren Rechner über die serielle Schnittstelle mit **X4100/200/300**, wie in Kapitel 3.4, Seite 46 beschrieben.
- Schalten Sie **X4100/200/300** aus und wieder ein.

  Nachdem **X4100/200/300** verschiedene Selbsttests durchgeführt hat, sehen Sie:
  "`Press <sp> for boot monitor or any other key to boot system`" z. B. im HyperTerminal.
- 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 **X4100/200/300** werden gelöscht.
- Wählen Sie "`(1) Boot System`".

  X4100/200/300 wird neu gestartet.
- Konfigurieren Sie **X4100/200/300** erneut.

Ich kann X4100/200/300 im LAN nicht erreichen.

- Überprüfen Sie mit dem MMI, ob Sie eine IP-Adresse eingetragen haben.

Wenn eine IP-Adresse eingetragen ist, dann versuchen Sie als nächstes eine serielle Verbindung herzustellen:

- Verbinden Sie Ihren Rechner über die serielle Schnittstelle mit **X4100/200/300**.
- 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 ***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 4.1.2, Seite 57). Wenn Sie die Standardeinstellungen im BOOTmonitor verändert haben, passen Sie Ihre Terminal-Einstellungen daran an.
- Wenn Sie keinen Erfolg haben, gehen Sie vor wie unter "Ich habe mein Paßwort vergessen.", Seite 391 beschrieben.

11.2.2 ISDN-Verbindungen

Hier finden Sie mögliche Fehlerquellen für ISDN-Verbindungen.

Die Telefonrechnung ist ungewöhnlich hoch.

Nutzen Sie die Funktion Taschengeldkonto (siehe Kapitel 9.1.3, Seite 321). Damit können Sie für Verbindungen mit **X4100/200/300** ein Limit festlegen, um Gebühren aufgrund von Fehlern bei der Konfiguration in Grenzen zu halten.

Möglicherweise gibt es auf **X4100/200/300** ISDN-Verbindungen, die ständig offen bleiben oder es werden ungewollte ISDN-Verbindungen aufgebaut, die zusätzliche Kosten verursachen.

- Überprüfen Sie mit `debug all` oder `trace`, ob ein Rechner im LAN eine andere Netzmaske verwendet als auf **X4100/200/300** eingetragen ist.
- Überprüfen Sie mit `debug all` oder `trace`, ob ein Rechner im LAN mit einer falschen IP-Adresse für Remote-CAPI konfiguriert ist (Ziel-Port 2662).
- Überprüfen Sie in ***System*** ➧ ***External System Logging***, ob **X4100/200/300** so konfiguriert ist, daß Syslog-Messages auf einen Host außerhalb des LANs geschickt werden (Ziel-Port 514).
- Überprüfen Sie in ***IP*** ➧ ***Static Settings***, ob für **X4100/200/300** unter **Time Server** eine IP-Adresse eingetragen wurde, die außerhalb des LANs liegt.
- Überprüfen Sie in der MIB-Tabelle **biboAdmTrapHostTable**, ob **X4100/200/300** so konfiguriert ist, daß SNMP-Traps auf einen Host außerhalb des LANs geschickt werden (Ziel-Ports 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 (Ziel-Ports 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 Client-Port aus auf Ziel-Port 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 Client-Port aus auf Ziel-Port 53 zugegriffen). Richten Sie eine lokale HOSTS-Datei im Windows-Verzeichnis ein, die die Namensauflösung durchführen kann.

- Überprüfen Sie mit `debug all` oder `trace`, ob auf einem Rechner im LAN "NetBIOS over IP" eingerichtet ist (es wird vom Source-Port 137 auf den Ziel-Port 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 9.2.8, Seite 339.
- Überprüfen Sie, ob Sie Callback konfiguriert haben (siehe Kapitel 9.2.4, Seite 331) 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 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 ***CALLS*** ➧ ***ADD*** die eigene Rufnummer richtig eingetragen ist. Sie gilt auch für ausgehende Rufe!

Eingehende Rufe kommen nicht zustande.

- 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** und **LocalCause** in der MIB-Tabelle **isdnCallHistoryTable**. Zur Interpretation der Einträge siehe **Software Reference**.
- Überprüfen Sie in ***CALLS***, 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.

12 Technische Daten

Allgemeine Produktmerkmale:

Bezeichnung	Wert
Abmessungen 19-Zoll-Einbaugerät	B x H x T in mm 220 x 44 x 290
Gewicht 19-Zoll-Einbaugerät	2,1 kg
Transportgewicht (inkl. Dokumentation, Kabel, Verpackung) 19-Zoll-Einbaugerät	4,6 kg
Umweltanforderungen: Lagertemperatur Betriebstemperatur Relative Luftfeuchtigkeit Raumklassifizierung	 -20 °C bis 50 °C 0 °C bis 40 °C 20 bis 90 % nicht kondensierend im Betrieb 5 bis 95 % nicht kondensierend bei Lagerung Nur in trockenen Räumen betreiben
Mitgelieferte gedruckte Dokumentation	Benutzerhandbuch

Tabelle 12-1: Technische Daten von **X4100/200/300**

12.1 Netzteil

Die Kaltgerätebuchse des Netzteils wird mit dem mitgelieferten Netzkabel an die Stromversorgung angeschlossen.

	Elektrische Anschlußwerte
Netzteil	Weitbereichsnetzteil ohne Lüfter
Netzspannung	100 bis 240 VAC
Netzfrequenz	50 bis 60 Hz
Max. Stromaufnahme	800 mA

Tabelle 12-2: Technische Daten des Netzteils

12.2 Leistungsmerkmale des Grundgeräts

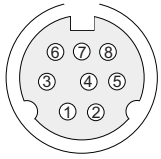
Die Leistungsmerkmale der Grundgeräte von **X4100**, **X4200** und **X4300** sind in der folgenden Tabelle aufgelistet:

Bezeichnung	Wert
Prozessor	Motorola MPC860T RISC CPU
Speicher	16 MB SDRAM 4 MB Flash-ROM
Schnittstellen:	
Konsolenschnittstelle (**X4100**, **X4200**, **X4300**)	Seriell, Mini-DIN
Ethernet/LAN-Schnittstelle (**X4100**, **X4200**, **X4300**)	10/100 Base-T Autosensing, RJ45-Buchse
10-BT-Ethernet-Schnittstelle (**X4100**, **X4200**)	RJ45-Buchse
ISDN-Schnittstelle BRI (**X4100**, **X4200**, **X4300**)	RJ45-Buchse
X.21/V.35-Schnittstelle (1x **X4200**, 2x **X4300**)	26-polige Mini-Delta-Ribbon-Buchse, bis 2048 kBit/s
Anzeigen	grün beleuchtetes 122 x 132-Pixel-LCD-Display mit beleuchteten Eingabetasten
Erweiterbarkeit	Steckplatz für eine **X4100/200/300**-Erweiterungskarte

Tabelle 12-3: Leistungsmerkmale der Grundgeräte

12.2.1 Serielle Konsolenschnittstelle

Die Pinbelegung der seriellen Konsolenschnittstelle des Grundgeräts (8-polige MiniDin-Buchse, **X4100**, **X4200** und **X4300**):

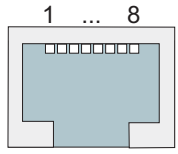


1	Für Testzwecke	5	RXD
2	Für Testzwecke	6	NC
3	TXD	7	NC
4	GND	8	NC

Bild 12-1: Pinbelegung der seriellen Konsolenschnittstelle für **X4100**, **X4200** und **X4300**

12.2.2 Ethernet/LAN-Schnittstelle

Die Pinbelegung der 10/100-Base-T-Ethernet/LAN-Schnittstelle des Grundgeräts (RJ45-Buchse, **X4100**, **X4200** und **X4300**):



1	T+	5	Schirm
2	T-	6	R-
3	R+	7	Schirm
4	Schirm	8	Schirm

Bild 12-2: 10/100-Base-T-Ethernet/LAN-Schnittstelle (RJ45-Buchse) des Grundgeräts mit Pinbelegung für **X4100**, **X4200** und **X4300**

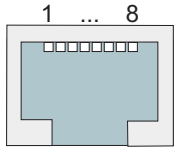
Das zu verwendende LAN-Kabel muß die folgenden technischen Merkmale erfüllen:

- 100-Base-T-Kabel CAT5 STP (Shielded Twisted Pair)
- Beidseitig vollständig abgeschirmter 8-poliger RJ45-Stecker
- Vier verdrillte Aderpaare zu je zwei Adern; folgende Adern sind verdrillt:
  - Pin 1+2
  - Pin 3+6
  - Pin 4+5
  - Pin 7+8

  Gesamtschirmung um alle vier Aderpaare.

12.2.3 10-BT-Ethernet-Schnittstelle für X4100 und X4200

Die Pinbelegung der 10-BT-Ethernet-Schnittstelle des Grundgerätes (RJ45-Buchse, **X4100** und **X4200**):



1	T+	5	Schirm
2	T-	6	R-
3	R+	7	Schirm
4	Schirm	8	Schirm

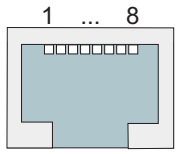
Bild 12-3: 10-BaseT-Ethernet-Schnittstelle (RJ45-Buchse) des Grundgeräts mit Pinbelegung für **X4100** und **X4200**

Das zu verwendende LAN-Kabel muß die folgenden technischen Merkmale erfüllen:

- 10-Base-T-Kabel CAT3 UTP (Unshielded Twisted Pair)
- 8-poliger RJ45-Stecker
- 2 verdrillte Aderpaare zu je 2 Adern; folgende Adern sind verdrillt:
  - Pin 1+2
  - Pin 3+6

12.2.4 ISDN-BRI-Schnittstelle

Die Pinbelegung der ISDN-BRI-Schnittstelle (RJ45-Buchse, **X4100**, **X4200** und **X4300**):



1	NC	5	R-
2	NC	6	T-
3	T+	7	NC
4	R+	8	NC

Bild 12-4: ISDN-BRI-Schnittstelle (RJ45-Buchse) des Grundgeräts mit Pinbelegung

12.2.5 Serielle WAN-Schnittstellen für X4200 und X4300

Das Grundgerät der **X4200** verfügt über eine, das Grundgerät der **X4300** über zwei serielle WAN-Schnittstellen:

Der serielle Port (Setup-Tool-Menü ***CM-SERIAL, SERIAL*** ➧ ***UNIT 0***) ist als Schnittstelle der folgenden Typen verwendbar:

- X.21/V.11
- V.35/V.11

Durch die Einstellung im Setup-Tool-Feld **Connector** (siehe Tabelle 6-11, Seite 137) kann der Port so umgestellt werden, daß **X4100/200/300** sowohl im DCE- als auch im DTE-Modus betrieben werden kann.

Durch entsprechende Einstellungen im Setup-Tool-Feld **Connector** werden physikalisch die Signalrichtung und Bedeutung der Pins umgedreht.

Die zu verwendenden Kabel sind nicht im Lieferumfang von **X4100/200/300** enthalten, können aber bei Ihrem Händler bestellt werden.

Wir empfehlen, Original-BinTec-Kabel zu verwenden, die Sie von Ihrem Händler beziehen können.

Die Verwendung von anderen Kabeln kann zur Beschädigung des Geräts und zum Garantieverlust führen!

Stecker Im folgenden werden zunächst die Stecker beschrieben, die für X.21 bzw. V.35 in der Regel verwendet werden:

- "DB-15-Stecker für X.21", Seite 405)
- "M34-Stecker für V.35", Seite 406)

Buchse Anschließend wird der serielle Port der Geräte **X4200** und **X4300** beschrieben, über den die X.21/V.35-Schnittstellen realisiert werden:

- "26-polige Mini-Delta-Ribbon-Buchse für X.21 und V.35 (X4200 und X4300)", Seite 407)

DB-15-Stecker für X.21

DB-15-Stecker für X.21

Für eine X.21-Schnittstelle wird in der Regel ein DB-15-Stecker nach ISO 4903 verwendet:

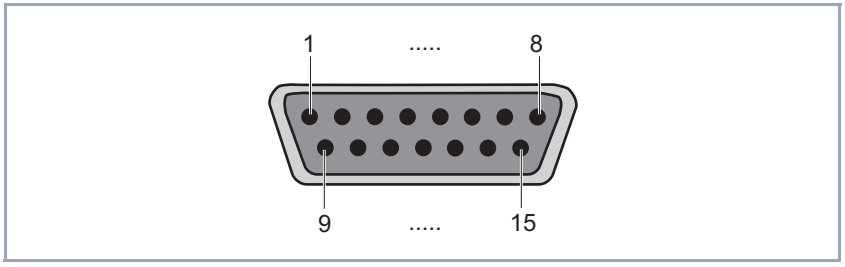


Bild 12-5: DB-15-Stecker (DTE)

Pinbelegung für DB-15-Stecker

Die Pins des DB-15-Steckers (DTE) bzw. -Buchse (DCE) sind folgendermaßen belegt:

Signal	Pin-Nr.	Quelle	Signalbeschreibung
	1		Schutzerde (Schirmung)
G	8		Signalerde
T (A) T (B)	2 9	DTE	Sendedaten
R (A) R (B)	4 11	DCE	Empfangsdaten
C (A) C(B)	3 10	DTE	Control
I (A) I (B)	5 12	DCE	Indication
S (A) S (B)	6 13	DCE	Sende- und Empfangstakt
X (A) X (B)	7 14	DTE	Sendetakt (Wird nur für das DCE-Kabel unterstützt)

Tabelle 12-4: Pinbelegung eines DB-15-Steckers für X.21 (ISO 4903)

M34-Stecker für V.35

M34-Stecker für V.35

Für eine V.35-Schnittstelle wird in der Regel ein M34-Stecker nach ISO 2593 verwendet:

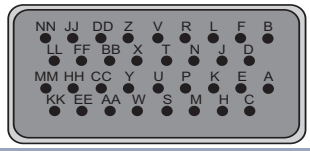


Bild 12-6: M34-Stecker

Pinbelegung für M34-Stecker

Die Pins des M34-Steckers sind folgendermaßen belegt:

ITU-T	Signal	Pin-Nr.	Quelle	Signalbeschreibung
		A		Schutzerde (Schirmung)
102	SG	B		Signalerde / Rückleiter
103	TD (A) TD (B)	P S	DTE	Sendedaten
104	RD (A) RD (B)	R T	DCE	Empfangsdaten
105	RTS	C	DTE	Request To Send
106	CTS	D	DCE	Clear To Send
107	DSR	E	DCE	Data Set Ready
108	DTR	H	DTE	Data Terminal Ready
109	DCD	F	DCE	Data Carrier Detect
113	TxC (A) TxC (B)	U W	DTE	Sendetakt - wird in Sonderfällen statt 114 verwendet
114	TxC (A) TxC (B)	Y AA	DCE	Sendetakt
115	RxC (A) RxC (B)	V X	DCE	Empfangstakt

Tabelle 12-5: Pinbelegung eines M34-Steckers für V.35 (ISO 2593)

Mini-Delta-Ribbon-Buchse für X.21 und V.35

26-polige Mini-Delta-Ribbon-Buchse für X.21 und V.35 (X4200 und X4300)

Die serielle X.21/V.35-Schnittstelle von **X4200** und **X4300** ist als 26-polige Mini-Delta-Ribbon-Buchse ausgeführt. Je nach Einstellung unter **Interface Type** kann die Schnittstelle für X.21 oder V.35 verwendet werden.

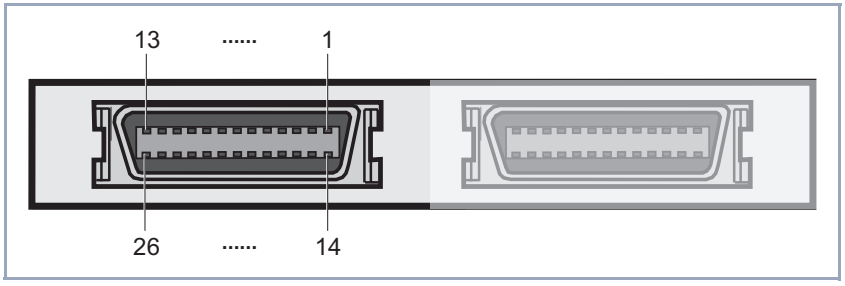


Bild 12-7: 26-polige Mini-Delta-Ribbon-Buchse (erster serieller Port, links)

Pinbelegung der Mini-Delta-Ribbon-Buchse

Die Pins der 26-poligen Mini-Delta-Ribbon-Buchse sind folgendermaßen belegt:

Signal	Pin-Nr.	X.21 (DB-15)		V.35 (M34)		V.36 (DB-37)		EIA-530 (DB-25)	
		DTE	DCE	DTE	DCE	DTE	DCE	DTE	DCE
Schirm	A1 (1)	1	1	A	A	1	1	1	1
GND	A2 (2)	8	8	B	B	19	19	7	7
TxD (B)	A3 (3)	9	11	S	T	22	24	14	16
TxD (A)	A4 (4)	2	4	P	R	4	6	2	3
RxD (B)	A5 (5)	11	9	T	S	24	22	16	14
RxD (A)	A6 (6)	4	2	R	P	6	4	3	2
RTS (B)	A7 (7)	10	12			25	27	19	13
RTS (A)	A8 (8)	3	5	C	D	7	9	4	5
CTS (B)	A9 (9)	12	10			27	25	13	19
CTS (A)	A10 (10)	5	3	D	C	9	7	5	4

Signal	Pin-Nr.	X.21 (DB-15)		V.35 (M34)		V.36 (DB-37)		EIA-530 (DB-25)	
		DTE	DCE	DTE	DCE	DTE	DCE	DTE	DCE
RxC (B)	A11 (11)	13	14	X	W	26	35	9	11
RxC (A)	A12 (12)	6	7	V	U	8	17	17	24
Mode DCE	A13 (13)		8		B		19		7
Mode 0	B1 (14)					19	19		
DTR (B)	B2 (15)					30	29	23	22
DTR (A)	B3 (16)			H	E	12	11	20	6
DCD (B)	B4 (17)					31	31	10	10
DCD (A)	B5 (18)			F	F	13	13	8	8
DSR (B)	B6 (19)					29	30	22	23
DSR (A)	B7 (20)			E	H	11	12	6	20
TxC (B)	B8 (21)			AA	AA	23	23	12	12
TxC (A)	B9 (22)			Y	Y	5	5	15	15
Mode 1	B10 (23)							7	7
Mode 2	B11 (24)	8	8						
TxCE (B)	B12 (25)		13	W	X	35	26	11	9
TxCE (A)	B13 (26)		6	U	V	17	8	24	17

Tabelle 12-6: Pinbelegung der 26-poligen Mini-Delta-Ribbon-Buchse

12.3 Leistungsmerkmale der Erweiterungs- und Ressourcenkarten

Dieses Kapitel umfaßt die technischen Daten für folgende Erweiterungskarten:

- X4E-2/3BRI, Kapitel 12.3.1, Seite 409
- X4E-1/2PRI, Kapitel 12.3.2, Seite 411
- X4E-2FE, Kapitel 12.3.3, Seite 413

Die technischen Daten der Ressourcenkarten (Digitale Modems, Verschlüsselung und Kompression) finden Sie in folgenden Kapiteln:

- XT-S/M/2M/L, Kapitel 12.3.4, Seite 414
- XT-ENC, Kapitel 12.3.5, Seite 415

12.3.1 X4E-2/3BRI – WAN-Schnittstellenkarte für ISDN-BRI (Basic Rate Interface)

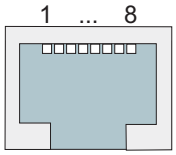
Die technischen Daten der X4E-2/3BRI-Erweiterungskarte:

Bezeichnung	Wert
Schnittstellen	3 x ISDN-Schnittstelle BRI S/T
Betriebstemperatur	0 °C bis 40 °C
Relative Luftfeuchtigkeit	20 bis 90 % nicht kondensierend im Betrieb 5 bis 95 % nicht kondensierend bei Lagerung
Erweiterungen	Steckplatz für Ressourcenkarte mit Digitalmodems Steckplatz für Ressourcenkarte zur Verschlüsselung und Kompression

Tabelle 12-7: Leistungsmerkmale der BRI-Erweiterungskarte

Pinbelegung ISDN-BRI-Schnittstelle der Erweiterungskarte

Die Pins der ISDN-BRI-Schnittstellen (RJ45-Buchsen) sind folgendermaßen belegt:



1	NC	5	R-
2	NC	6	T-
3	T+	7	NC
4	R+	8	NC

Bild 12-8: ISDN-BRI-Schnittstelle (RJ45-Buchse) der BRI-Erweiterungskarte

12.3.2 X4E-1/2PRI – WAN-Schnittstellenkarte für ISDN-PRI (Primary Rate Interface) und/oder G.703

Die technischen Daten der X4E-1/2PRI-Erweiterungskarte:

Bezeichnung	Wert
Schnittstellen	2 x Schnittstelle für ISDN-PRI/G.703 mit jeweils 2 Buchsen (IN und OUT) Beim Abschalten von **X4100/200/300** wird Buchse IN auf Buchse OUT durchgeschleift.
Datenkompression und Verschlüsselung	Integrierte Hardware-Unterstützung für Verschlüsselung und Kompression
Betriebstemperatur	0 °C bis 40 °C
Relative Luftfeuchtigkeit	20 bis 90 % nicht kondensierend im Betrieb 5 bis 95 % nicht kondensierend bei Lagerung
Erweiterungen	2 x Steckplatz für Ressourcenkarte mit Digitalmodems

Tabelle 12-8: Leistungsmerkmale der PRI/G.703-Erweiterungskarte

Pinbelegung ISDN-PRI-Schnittstelle der Erweiterungskarte

Grafische Darstellung der ISDN-PRI/G.703-Schnittstelle:

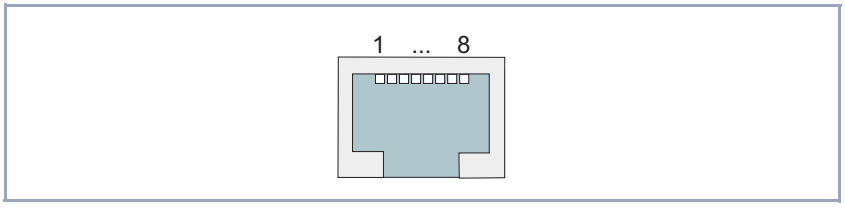


Bild 12-9: ISDN-PRI/G.703-Schnittstelle (RJ45-Buchse) der PRI/G.703-Erweiterungskarte

Die Pins der ISDN-PRI/G.703-Schnittstelle sind folgendermaßen belegt:

Pin	Funktion	Bezeichnung auf NT
1	Empfangen (Receive), NT zu TE (+)	S2Mab/a

Pin	Funktion	Bezeichnung auf NT
2	Empfangen (Receive), NT zu TE (–)	S2Mab/b
3	Nicht genutzt	
4	Senden (Transmit), TE zu NT (+)	S2Man/a
5	Senden (Transmit), TE zu NT (–)	S2Man/b
6-8	Nicht genutzt	

Tabelle 12-9: Pinbelegung der ISDN PRI/G.703-Schnittstelle (RJ45-Buchse)

Wir empfehlen, bei der Installation des NT (Network Terminator) an dem S_{2M}-Anschluß einen Stecker mit der in Tabelle 12-9, Seite 412 angegebenen Pinbelegungen für "Emfpangen" und "Senden" zu verwenden. Dadurch wird eine korrekte Verbindung zur PRI-Schnittstelle des Routers mit dem mitgelieferten Kabel sichergestellt.

Beachten Sie außerdem, daß der NT eine getrennte Stromversorgung von 60 V benötigt. Die Firma, die die Installation Ihres NTs vornimmt, sollte darauf hingewiesen werden, daß diese separate Stromversorgung installiert werden muß, da diese nicht von dem Endgerät (gewöhnlich PBX für S_{2M}-Schnittstellen) gestellt wird.

Hinweis für NTs in Deutschland

In Deutschland wird "Senden" (NT-->TE) oft mit "S2Mab" (a und b) auf dem Anschlußstecker benannt, "Empfangen" (TE-->NT) mit "S2Man" (a und b).

Auf dem NT befinden sich gewöhnlich mehrere LEDs, die den jeweiligen Status anzeigen. Die Angaben in Tabelle 12-10, Seite 413 scheinen größtenteils standardisiert zu sein. Im Zweifelsfalle konsultieren Sie bitte die Bedienungsanleitung Ihres NTs:

LED	Bezeichnung	Bedeutung
1: Farbe Grün	NT	LED an: Zeigt gewöhnlich an, daß die richtige Spannung anliegt.

LED	Bezeichnung	Bedeutung
2: Farbe Rot	UK2	LED an (oder blinkend): Zeigt gewöhnlich an, daß die S_{2M}-Schnittstelle an der Vermittlungsstelle nicht aktiviert wurde. In diesem Fall muß Ihre Telefongesellschaft die Schnittstelle aktivieren.
3: Farbe Rot	S2M	LED an: Zeigt gewöhnlich an, daß die Signale nicht vom Endgerät empfangen werden.

Tabelle 12-10: NT-LEDs und ihr Status

12.3.3 X4E-2FE – LAN-Schnittstellenkarte für 10/100 MBit/s

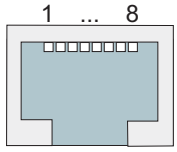
Die technischen Daten der X4E-2FE-Erweiterungskarte:

Bezeichnung	Wert
Schnittstellen	2 x 10/100 Base-T Autosensing
Betriebstemperatur	0 °C bis 40 °C
Relative Luftfeuchtigkeit	20 bis 90 % nicht kondensierend im Betrieb 5 bis 95 % nicht kondensierend bei Lagerung
Erweiterungen	Steckplatz für Ressourcenkarte zur Verschlüsselung und Kompression

Tabelle 12-11: Leistungsmerkmale der LAN-Erweiterungskarte

Pinbelegung LAN-Schnittstelle der Erweiterungskarte

Die Pins der LAN-Schnittstellen (RJ45-Buchsen) sind folgendermaßen belegt:



1	T+	5	Schirm
2	T-	6	R-
3	R+	7	Schirm
4	Schirm	8	Schirm

Bild 12-10: LAN-Schnittstelle (RJ45-Buchse) der LAN-Erweiterungskarte

12.3.4 XT-S/M/2M/L – Ressourcenkarten mit Digitalmodems

Die Ressourcenkarten mit Digitalmodems sind in folgenden Aufsführungen für X4E-3BRI und X4E-2PRI erhältlich:

Achtung!

Der Einbau von Ressourcenkarten in eine Erweiterungskarte führt zu verstärkter Wärmeentwicklung. Um die Schädigung von Bauteilen zu vermeiden, ist der Einsatz einer Lüfterkassette zwingend erforderlich!

➤ Setzen Sie bei Verwendung einer Erweiterungskarte mit Ressourcenkarte(n) im **X4100/200/300**-Einbaugerät die Lüfterkassette ein.

Sie können die Lüfterkassette von Ihrem Lieferanten käuflich erwerben.

- XT-S mit 8 Digitalmodems
- XT-M mit 12 Digitalmodems
- XT-2M mit 24 Digitalmodems
- XT-L mit 30 Digitalmodems

Technische Daten der Ressourcenkarten:

Bezeichnung	Wert
Betriebstemperatur	0 °C bis 40 °C
Relative Luftfeuchtigkeit	20 bis 90 % nicht kondensierend im Betrieb 5 bis 95 % nicht kondensierend bei Lagerung

Tabelle 12-12: Leistungsmerkmale der Ressourcenkarten mit Digitalmodems

12.3.5 XT-ENC – Ressourcenkarte zur Verschlüsselung und Kompression

Die Ressourcenkarten zur Verschlüsselung und Kompression bietet eine Hardware-Unterstützung für STAC-Kompression und symmetrische Verschlüsselung. Unterstützte Verschlüsselungsverfahren: DES, 3DES, CAST und Blowfish.

Achtung!

Der Einbau von Ressourcenkarten in eine Erweiterungskarte führt zu verstärkter Wärmeentwicklung. Um die Schädigung von Bauteilen zu vermeiden, ist der Einsatz einer Lüfterkassette zwingend erforderlich!

➤ Setzen Sie bei Verwendung einer Erweiterungskarte mit Ressourcenkarte(n) im **X4100/200/300**-Einbaugerät die Lüfterkassette ein.

Sie können die Lüfterkassette von Ihrem Lieferanten käuflich erwerben.

Bezeichnung	Wert
Betriebstemperatur	0 °C bis 40 °C
Relative Luftfeuchtigkeit	20 bis 90 % nicht kondensierend im Betrieb 5 bis 95 % nicht kondensierend bei Lagerung

Tabelle 12-13: Leistungsmerkmale der Ressourcenkarte zur Verschlüsselung und Kompression

Die ISDN-PRI- bzw. G.703-Erweiterungskarte ist im Auslieferungszustand mit Hardware-Unterstützung für Verschlüsselung und Kompression ausgestattet.

Die ISDN-BRI-Erweiterungskarte sowie die LAN-Erweiterungskarte können optional mit einer entsprechenden Ressourcenkarte ausgestattet werden.

Aufgrund von Export- bzw. Importbestimmungen kann die Lieferung der Ressourcenkarten zur Verschlüsselung und Kompression nicht immer gewährleistet werden.

13 Wichtige Kommandos

Dieses Kapitel beschreibt folgende Kommandos:

- SNMP-Shell-Kommandos:
  - telnet
  - ping
  - trace
  - isdnlogin
  - debug
  - ifconfig
  - ifstat
  - netstat
  - date
  - t
  - nslookup
- BRICKtools-for-Unix-Kommandos:
  - bricktrace
  - capitrace

13.1 SNMP-Shell-Kommandos

Auf **X4100/200/300** 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:

Durch Eingabe von ? wird eine Übersicht der wichtigsten Kommandos angezeigt, die auf **X4100/200/300** verfügbar sind

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 [-i] [-f <precount>] [-d <msec>] [-c <count>] <target>
[<size>]
```

Wird benutzt, um die Kommunikation mit einem anderen Host zu testen.

- `-i:` Schickt jedes Paket um ein Byte vergrößert.
- `-f <precount>:` Zunächst werden <precount> Pakete geschickt. Das nächstes Paket wird geschickt, sobald ein Paket empfangen wurde.

Output: für jedes geschickte Paket erscheint ein Punkt auf dem Bildschirm, für jedes empfangene Paket wird ein Punkt gelöscht.
Mit `-f 1` und ohne zusätzliche Angabe von `-d <msec>` wird ca. die Hälfte der Bandbreite des Geräts mit Senden bzw. Empfangen von Paketen ausgelastet.

- `-d <msec>:` wartet `<msec>` Millisekunden bis nächstes Paket geschickt wird, default: 1000 Millisekunden
- `-c <count>`: Limitiert die Anzahl der gesendeten Pakete, `<count>` Pakete werden gesendet.
- `target`: 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 [-h23aFADtpiNxX] [-T <tei>] [-c <cref>]
[<channel> <unit> <slot> | next | <ifcname>]
```

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).
- `-D`: Zusätzliche Zeitangabe (Delta)
- `-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).
- `-T <tei>`: TEI-Filter setzen (nur D-Kanal).
- `-c <cref>`: Callref-Filter setzen (nur D-Kanal).
- `channel`: 0 = D-Kanal, X.21-Schnittstelle oder Ethernet, 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.
- `next`: Nur Informationen über den als nächstes geöffneten B-Kanal anzeigen.
- `<ifcname>`: Name oder Index der Schnittstelle (siehe "ifstat", Seite 422).
- `-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.
- spezielle `<MAC filter>`: `me` = **X4100/200/300**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 **X4100/200/300** zu öffnen.

- `-c <stknumber>`: Definiert den ISDN-Stack (falls mehrere ISDN-Karten genutzt werden)
- `-C`: Versucht, Komprimierung (V.42bis) anzuwenden.
- `-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]|[[-q] all|acct|system|<subs> [<subs> ...]]
```

Wird benutzt, um ausgewählte Debugging-Informationen von **X4100/200/300**s Subsystemen anzuzeigen.

- `show`: Alle möglichen Subsysteme anzeigen, die auf Fehler untersucht werden können.
- `-q`: Keinen 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 für 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>]
```

Weist der Schnittstelle `<interface>` die IP-Adresse und die zugehörige Netzmaske zu und konfiguriert die zugehörigen Parameter. Die Routing-Tabelle wird entsprechend geändert.

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`: **X4100/200/300**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 zwölften 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]
```

X4100/200/300 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 (im Auslieferungszustand wird eine Verbindung zu **X4100/200/300** über Telnet, ISDN-Login 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.

nslookup

```
nslookup [-an] [-t <type>] [-w <sec>] [-r <ret>] ipaddr |
name [<server>]
```

Wird benutzt, um zu prüfen, wie ein Name oder eine IP-Adresse durch **X4100/200/300** oder einen anderen Name-Server aufgelöst wird.

- `-a`: Zeigt alle erhaltenen Daten an.
- `-n`: Verhindert die Auflösung der angegebenen Name-Server-Adresse (ohne diese Option wird versucht, die Adresse des Name-Servers aufzulösen).
- `-t <type>`: Anfragen der Art <type> ausführen. Mögliche Werte für type: 0, A, NS, MD, MF, CNAME, SOA, MB, MG, MR, NULL, WKS, PTR, HINFO, MINFO, MX, TXT, ANY oder eine beliebige Dezimalzahl.
- `-w <sec>`: `<sec>` Sekunden warten, bevor eine Anfrage erneut gesendet wird (Standardwert: 3).
- `-r <ret>`: Höchstens `<ret>` mal eine Anfrage senden (Standardwert: 5).
- `ipaddr`: Aufzulösende IP-Adresse.
- `name`: Aufzulösender Name.
- `<server>`: IP-Adresse des Name-Servers, der befragt werden soll (Standardwert: 127.0.0.1). Es wird versucht, diese Name-Server-Adresse vom lokalen DNS-Proxy auflösen zu lassen.

Durch Eingabe von `-?` erhalten Sie gewöhnlich Hilfen zur Syntax.

Das Kommando `update` finden Sie in Kapitel 10.2, Seite 382.

Weitere SNMP-Kommandos finden Sie in der **Software Reference**.

13.2 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).
- `-t`: Ausgabe in ASCII-Text (nur B-Kanal).
- `-x`: Raw dump mode.
- `-s`: **X4100/200/300** 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 Schnittstelle für Module mit zwei Schnitstellen (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 **X4100/200/300** gesendeten oder empfangenen CAPI-Meldungen werden angezeigt. Als Umgebungsvariable CAPI_HOST muß die IP-Adresse von **X4100/200/300** eingegeben werden.

- `-h`: Hexadezimale Ausgabe.
- `-s`: Kurze Ausgabe. Am Ende der Informationszeile wird lediglich die Applikations-ID, ein "connection 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 ([<decimal>])
- Applikations-ID (ID = <decimal>)
- Nummer der CAPI-Meldung (no (<decimal>))
- Nur bei Kurzer Ausgabe: Connection-Identifier (ident = 0x<hexadecimal>

14 Allgemeine Sicherheitshinweise in 15 Landessprachen

General Safety Precautions in English

The following sections contain safety precautions you are strongly advised to heed when working with your equipment.

Transport and storage

- Only transport and store **X4100/200/300** in its original packaging or use other appropriate packaging to protect against knocking and shaking.

Installation and operation

- Read the information on the ambient conditions (see Technical Data) before installing and operating **X4100/200/300**. Place the equipment on a firm flat base.
- Electrostatic charges may cause damage to the equipment. You should therefore wear a grounded wrist strap or touch a grounded surface before you touch sockets or extension cards of **X4100/200/300**. Only grip extension cards at the edges and do not touch components or conductor tracks.
- Keep the unused extension slot covered with the dummy cover to prevent objects getting inside the equipment. Foreign bodies located in the equipment during operation create a danger of electric shock and short-circuits.
- Ensure that no sharp objects can damage the window of the display module. Protect the display module against knocks and dropping and only connect it to the RJ11 socket provided for this purpose on **X4100/200/300** to prevent damage to **X4100/200/300** and the display module.
- Make sure the cables do not cover the ventilation slots of the equipment or interfere with ventilation. Obstructing the ventilation of **X4100/200/300** may cause damage to the equipment. Damage caused by lack of ventilation invalidates the guarantee.
- Never open the basic unit or tamper with the mains unit in any way, as this can create a lethal danger through electric shock. Don’t remove any fixing screws on the basic unit.
- Condensation may occur externally or internally if the equipment is moved from a colder room to a warmer room. When moving the equipment under

such conditions, allow ample time for the equipment to reach room temperature and to dry out completely before operating. Observe the ambient conditions under Technical Data.

- Make sure the local mains voltage is the same as the nominal voltages of the mains unit. The equipment may only be operated under the following conditions.
  - 100 - 240 V AC
  - 50/60 Hz
- Make sure the safety mains socket in the building is freely accessible. You must remove the mains plug to disconnect the equipment completely from the mains.
- Make sure you follow the correct cabling sequence, as described in the manual. Use only the cables supplied with the equipment or cables that meet the specifications in this manual. If you use other cables, BinTec Access Networks GmbH cannot accept liability for any damage occurring or for any adverse effects on operation. The equipment guarantee is invalidated in such cases.
- Connect the equipment as described in the manual.
- Arrange the cables so that they are not in the way and cannot be tripped over or damaged.
- Do not connect, disconnect or touch the data lines during lightning storms.

Operation according to the regulations

- **X4100/200/300** is intended for use in offices. As an ISDN multiprotocol router, **X4100/200/300** establishes WAN connections depending on the system configuration. To avoid extra charges, you should carefully monitor the product.
- **X4100/200/300** meets the relevant safety standards for information technology equipment for use in offices.
- Operation of the system according to IEC 950/EN 60950 is only guaranteed when the top of the housing is fitted (cooling, fire protection, RFI suppression).
- Ambient temperature should not exceed 50 °C. Avoid exposure to direct sunlight.

- Make sure no foreign objects (e.g. paper clips) or liquids get into the equipment (risk of electric shock, short-circuit). Make sure the equipment is sufficiently cooled.
- **X4100/200/300** contains no components for the user to replace or any switches or jumpers that need to be set by the user.
- In an emergency (e.g. damaged housing or operating element, entry of liquid or foreign bodies), immediately disconnect the power supply and notify customer service.

Cleaning and repair

- The equipment should only be opened by service centers authorized by BinTec. Always disconnect the power cord before opening the equipment. Unauthorized opening and improper repairs can result in serious danger for the user (e.g. electric shock). Ensure that repairs are only carried out by service centers authorized by BinTec. Your dealer will tell you where the service centers are situated. Failure to observe the above instructions invalidates the guarantee and no claims can be accepted.
- Never use water to clean this equipment. Water spillage can result in serious danger for the user (e.g. electric shock) and cause considerable damage to the equipment.
- Never use scouring or abrasive alkaline cleaning agents on this equipment.

Yleiset turvallisuusmääräykset

Seuraavista kappaleista löydät turvallisuusmääräykset, joita on ehdottomasti noudatettava reittivalitsinta käytettäessä.

Kuljetus ja varastointi

- Kuljeta ja varastoi **X4100/200/300** vain alkuperäispakkauksessaan tai muussa sopivassa pakkauksessa, joka suojaa töytäisyiltä ja iskuilta.

Asennus ja käyttöönotto

- Tarkista ennen **X4100/200/300** -laitteen asennusta ja käyttöä, että ympäristöolosuhteista annettuja ohjeita (kts. lukua Tekniset tiedot) on noudatettu. Aseta laite tukevalle, tasaiselle alustalle.
- Sähköstaattiset varaukset voivat johtaa laitteen vioittumisen. Pidä siksi ranteen ympärillä maadoitettua ranneketta tai kosketa maadoitettua pintaa, ennen kuin kosket **X4100/200/300**:n liittimiä tai laajennuskortteja. Kosketa laajennuskortteja periaatteessa vain reunoista äläkä tartu rakenneosiin tai johdinratoihin.
- Pidä käyttämättömät laajennuskorttipaikat suojuksilla suljettuina, jotta mitkään esineet eivät voi joutua laitteen sisälle. Jos laitteessa on käytön aikana vieraita esineitä, siitä aiheutuu sähköisku- ja oikosulkuvaara.
- Huolehdi siitä, että mitkään terävät esineet eivät vahingoita näyttömodulin ikkunaa. Suojaa näytömoduli iskuja ja putoamista vastaan. Liitä se vain **X4100/200/300**:n tähän tarkoitukseen varattuun RJ11-liittimeen **X4100/200/300**:n ja näyttömodulin vaurioitumisen välttämiseksi.
- Huomaa kaapeloitaessa, että laitteen tuuletusraot eivät peity ja tuuletus ei esty. **X4100/200/300**:n tuuletuksen estyessä laitteeseen voi syntyä vaurioita. Puutteellisesta tuuletuksesta aiheuneet vauriot johtavat takuun raukeamiseen.
- Älä avaa peruslaitetta äläkä muuntele verkkolaitetta mitenkään, sillä siitä aiheutuu sähköisku- ja hengenvaara. Älä poista yhtää kiinnitysruuvia peruslaitteesta.
- Kun laite tuodaan kylmästä ympäristöstä käyttötiloihin, sen ulko- sekä sisäpinnoille voi syntyä kastetta. Odota, että laitteen lämpötila on asettunut ja laite on ehdottoman kuiva, ennen kuin otat sen käyttöön. Huomioi ympäristövaatimukset, jotka on esitetty teknisissä tiedoissa.

- Tarkista, vastaako paikallinen verkkojännite verkkolaitteen nimellisjännitteitä. Laitetta saa käyttää seuraavissa olosuhteissa:
  – 100 - 240 VAC
  – 50/60 Hz
- Varmista, että suko-pistorasia on asennusta varten vapaasti tavoitettavissa. Verkkopistoke on vedettävä pistorasiasta laitteen irrottamiseksi täydellisesti verkosta.
- Huomaa kaapeloitaessa käsikirjassa kuvailtu järjestys. Käytä vain kaapelia, joka vastaa tämän käsikirjan spesifikaatioita tai joka toimitettiin alunperin laitteen mukana. Jos käytät toista kaapelia, BinTec Access Networks GmbH ei ota vastuuta vahingoista tai toiminnan huonontumisesta. Tällaisissa tapauksissa laitetakuu raukeaa.
- Noudata laitetta liittäessäsi käsikirjan ohjeita.
- Vedä kaapelit sellaisiin paikkoihin, että ne eivät aiheuta vaaratilanteita (kompastumisia) eivätkä vahingoitu.
- Älä liitä, irrota tai kosketa tiedonsiirtokaapeleita ukonilman aikana.

Määräystenmukainen käyttö, käyttö

- **X4100/200/300** on tarkoitettu käytettäväksi toimistoympäristössä. **X4100/200/300** on moniprotokollareititin, jonka avulla voidaan luoda järjestelmäkonfiguraatiosta riippuen WAN-yhteyksiä. Jotta ei-toivotuilta maksuilta vältytään, laitetta tulee ehdottomasti valvoa.
- **X4100/200/300** vastaa toimistotiloissa käytettäville tietotekniikan laitteistoille asetettuja asiaankuuluvia turvallisuusmääräyksiä.
- Järjestelmän IEC 950/EN 60950 mukainen käyttö on taattu ainoastaan, mikäli peltikotelo on asennettu täydellisesti (jäähdytys,palosuoja, kipinäsuoja).
- Ympäristön lämpötila ei saa nousta yli 50 °C:een. Vältä suoraa auringonpaistetta.
- Varo, ettei mitään vieraita esineitä (esim. paperiliittimiä) tai nesteitä pääse laitteen sisäpuolelle (sähköisku, lyhytsulku). Huolehdi siitä, että laitteen jäähdytys on riittävä.

- **X4100/200/300** :ssa ei ole mitää rakenneosia, jotka täytyy vaihtaa. Laitteessa ei ole myöskään kytkimiä tai jumppereita, jotka käyttäjän täytyy säätää.
- Keskeytä hätätilanteessa (esim. särkynyt kotelo tai käyttölaite, nesteen tai vieraiden esineiden joutuminen laitteen sisään) virransyöttö välittömästi ja ota yhteyttä huoltopalveluun.

Puhdistus ja korjaus

- Vain BinTec:in valtuuttama huoltokorjaamo saa avata laitteen. Verkkopistoke on ehdottomasti vedettävä seinästä ennen laitteen aukaisemista. Asiaton aukaiseminen ja asiantuntemattomat korjaukset voivat aiheuttaa käyttäjälle huomattavia vaaroja (esim. sähköisku). Anna vain BinTec:in valtuuttaman huoltokorjaamon korjata laitetta. Huoltokorjaamoa koskevia tietoja saat laitemyyjältäsi. Muissa tapauksissa kaikkinaiset takuuvaatimukset evätään.
- Älä missään tapauksessa puhdista laitetta runsaalla vedellä. Sen sisään tunkeutunut vesi saattaisi aiheuttaa vakavia vaaroja (esim. 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 **X4100/200/300** uniquement dans son emballage d'origine ou 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 **X4100/200/300**, veuillez vous référer aux indications concernant les conditions d'environnement (cf. Caractéristiques techniques). Utilisez un support stable et plat.
- Des charges électrostatiques peuvent endommager l'appareil. Il est donc important que vous portiez un bracelet antistatique ou que vous touchiez une surface mise à la terre avant de saisir des prises ou des cartes d'extension de **X4100/200/300**. Il est impératif de ne saisir les cartes d'extension que par les bords et de ne pas toucher aux composants ni aux circuits conducteurs.
- Refermez les emplacements des cartes d'extension non utilisés avec des caches borgnes de manière à ce que rien ne puisse pénétrer à l'intérieur de l'appareil. Si des objets se trouvent à l'intérieur de l'appareil en fonctionnement, il y a risque d'électrocution et de court-circuit.
- Veillez à ce qu'aucun objet pointu n'endommage la fenêtre du module d'affichage. Protégez le module d'affichage contre les chocs et les chutes ; ne le raccordez qu'à la prise RJ11 **X4100/200/300** prévue à cet effet, afin d'éviter tout dommage du **X4100/200/300** et du module d'affichage.
- Lors du câblage, veillez à ne pas recouvrir les fentes d'aération de l'appareil de manière à ne pas entraver la ventilaton. Le droit de garantie est annulé lorsque les dommages résultent d'une ventilation insuffisante.
- N'ouvrez pas l'appareil de base et n'effectuez aucune manipulation sur le bloc d'alimentation, sous risque de danger de mort par électrocution. Ne retirez aucune vis de fixation sur l'appareil de base.
- Si l'appareil est transporté dans une pièce où la température est plus élevée que celle de l'endroit d'où il provient, de la condensation risque de se former à l'extérieur comme à l'intérieur de l'appareil. Avant de mettre votre

appareil en service, attendez qu'il soit à la même température que celle de la pièce et qu'il soit absolument sec. Veuillez respecter les indications concernant les conditions d'environnement (cf. Caractéristiques techniques).

- Vérifiez si la tension secteur locale correspond aux tensions nominales du bloc d'alimentation. L'appareil ne devra fonctionner que dans les conditions ci-après :
  – 100 - 240 Vca
  – 50/60 Hz
- Vérifiez si la prise de courant de sécurité pour l'installation est librement accessible. Il faut retirer la fiche de contact pour garantir la déconnexion du secteur.
- Lors du câblage, respectez les étapes indiquées dans le manuel. N'utilisez que les câbles correspondants aux spécifications indiquées dans ce manuel ou les câbles d'origine joints lors de la livraison. Dans le cas où vous utiliseriez d'autres câbles que ces derniers, la société BinTec Access Networks GmbH décline toute responsabilité pour des dommages éventuels ou pour tout défaut de fonctionnement pouvant en résulter. Dans de tels cas, la garantie est annulée.
- Pour le raccordement de l'appareil, respectez les indications du manuel.
- Posez les câbles de telle sorte qu'ils ne puissent pas être à l'origine de risques (risques de trébuchement) ou être endommagés.
- Pendant un orage, ne connectez pas les lignes de transmission des données, ne les débranchez pas et ne les touchez pas.

Utilisation conforme, fonctionnement

- **X4100/200/300** est conçu pour l'utilisation dans les bureaux. En tant que router multiprotocole, **X4100/200/300** établit les connexions WAN en fonction de la configuration existante. Pour éviter des frais de taxation indésirables, il est impératif de placer ce produit sous contrôle.
- **X4100/200/300** est conforme aux prescriptions de sécurité relatives aux équipements de la technique de l'information pour l'utilisation dans les bureaux.

- Le fonctionnement de ce système conformément aux normes CEI 950/ EN 60950 ne peut être garanti que si le boîtier métallique est complètement monté (refroidissement, protections anti-incendie et antiparasite).
- La température ambiante ne doit pas dépasser 50 °C. Evitez le rayonnement direct du soleil sur l'appareil.
- Veillez à ce qu'aucun objet (des agrafes par exemple) ni aucun liquide ne s'introduise à l'intérieur de l'appareil (risque d'électrocution ou de court-circuit). Veillez à ce que l'appareil ait suffisamment refroidi.
- **X4100/200/300** ne contient aucun composant devant être remplacé par l'utilisateur et aucun commutateur/fil volant ayant besoin d'être réglé.
- Dans les cas d'urgence extrême (si le boîtier ou des éléments de commande sont endommagés, lorsque du liquide ou des corps étrangers se sont introduits dans l'appareil, par exemple), déconnectez immédiatement l'alimentation en courant et contactez le service après-vente.

Nettoyage et réparations

- L'appareil doit être ouvert uniquement par un point de service après-vente agréé par BinTec. Il est impératif de retirer la fiche secteur avant d'ouvrir l'appareil. L'ouverture non autorisée de l'appareil ainsi que des réparations non conformes exposent l'utilisateur à des risques graves (risque d'électrocution par exemple). Les réparations ne doivent être exécutées que un point de service après-vente agréé par BinTec. Votre concessionnaire vous fera part de l'adresse à laquelle vous pourrez contacter le service après-vente. Tout autre cas annule le droit à la garantie.
- L'appareil ne doit être en aucun cas nettoyé à l'eau. Une pénétration d'eau dans l'appareil pourrait entraîner des risques graves pour l'opérateur (risque d'électrocution par exemple) et des dommages importants de l'appareil.
- Ne jamais utiliser de produits récurants, de produits de nettoyage alcalins, ni d'outils tranchants ou grattants.

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 **X4100/200/300** μόνο στη γνήσια συσκευασία ή σε μία άλλη κατάλληλη συσκευασία, η οποία να εξασφαλίζει προστασία από τις κρούσεις και τα χτυπήματα.

Εγκατάσταση και έναρξη της λειτουργίας

- Πριν την εγκατάσταση και την έναρξη της λειτουργίας του **X4100/200/300** να λάβετε υπ' όψιν σας τις οδηγίες σχετικά με τις συνθήκες περιβάλλοντος (βλέπε Τεχνικά στοιχεία). Χρησιμοποιήστε ένα σταθερό και επίπεδο υπόβαθρο.
- Ηλεκτροστατικά φορτία μπορούν να προκαλέσουν βλάβη στη συσκευή. Γι αυτό, πριν έρθετε σε επαφή με τις υποδοχές ή της πλατίνες αναβάθμισης του **X4100/200/300** θα πρέπει να φοράτε ένα αντιστατικό μανικέτι γύρω από το χέρι σας ή να αγγίζετε μία γειωμένη επιφάνεια. Αγγίζετε τις πλατίνες αναβάθμισης μόνο στις άκρες και μη πιάνετε καλώδια η εξαρτήματα.
- Να διατηρείτε κλειστές τις μη χρησιμοποιημένες υποδοχές αναβάθμισης με το τυφλό κάλυμμα, ώστε να μην μπορούν να εισέλθουν αντικείμενα στο εσωτερικό της συσκευής. Αν κατά την διάρκεια της λειτουργίας υπάρχουν μέσα στην συσκευή ξένα αντικείμενα υπάρχει κίνδυνος ηλεκτροπληξίας και βραχυκυκλώματος.
- Να προσέχετε ώστε η οθόνη της μονάδας ενδείξεων να μην υποστεί ζημιές από αιχμηρά αντικείμενα. Να προστατεύετε την μονάδα ενδείξεων από χτυπήματα και πτώσεις και να την συνδέετε μόνον στην προβλεπόμενη υποδοχή RJ11 του **X4100/200/300**, για να αποφύγετε τις ζημιές στο **X4100/200/300** και στην μονάδα ενδείξεων.
- Κατά την καλωδίωση προσέξτε ώστε να μην καλύπτονται οι σχισμές εξαερισμού της συσκευής και να μην εμποδίζεται ο αερισμός. Από τον μειωμένο αερισμό του **X4100/200/300** μπορούν να προκληθούν ζημιές στην συσκευή. Οι βλάβες που προκύπτουν από ελλιπή αερισμό συνεπάγονται την απώλεια της εγγύσης.

- Μη ανοίγετε τη βασική συσκευή και μην κάνετε μετατροπές στον ρευματολήπτη, διότι υπάρχει κίνδυνος θάνατος απο ηλεκτροπληξία. Μη βγάζετε της βίδες στερέωσης της βασικής συσκευής.
- Όταν η συσκευή μεταφέρεται από ψυχρό περιβάλλον στον χώρο λειτουργίας μπορεί να παρουσιασθεί τήξη τόσο στο εξωτερικό όσο και στο εσωτερικό της συσκευής. Πριν την θέσετε σε λειτουργία περιμένετε μέχρι που η συσκευή να αποκτήσει την ίδια θερμοκρασία και να είναι τελείως στεγνή. Προσέξτε τις συνθήκες περιβάλλοντος στο Τεχνικά στοιχεία.
- Εξετάστε αν η τάση του τοπικού ηλεκτρικού δικτύου συμφωνεί με την ονομαστική τάση του ρευματολήπτη. Η λειτουργία της συσκευής επιτρέπεται μόνο με τις ακόλουθες προϋποθέσεις:
  - 100 - 240 VAC
  - 50/60 Hz
- Βεβαιωθείτε πως η πρίζα σούκο της εγκατάστασης είναι προσιτή. Για την πλήρη αποσύνδεση από το ρεύμα πρέπει να βγάζετε το φις από την πρίζα.
- Κατά την καλωδίωση προσέξτε την σειρά που περιγράφεται στο εγχειρίδιο. Να χρησιμοποιείτε μόνον καλώδια που πληρούν τα χαρακτηριστικά στο εγχειρίδιο ή τα γνήσια που παραλάβατε. Αν χρησιμοποιείτε άλλα καλώδια, τότε η BinTec Access Networks GmbH δεν αναλαμβάνει καμία ευθύνη για ζημιές ή βλάβες στην λειτουργικότητα. Σε αυτές τις περιπτώσεις παύει να ισχύει η εγγύηση της συσκευής.
- Κατά την σύνδεση της συσκευή λάβετε υπόψη σας τις υποδείξεις στο εγχειρίδιο.
- Διαστρώστε τα καλώδια κατά τέτοιον τρόπο, ώστε να μην προκύψουν σημεία κινδύνου (κίνδυνος παραπατήματος) και ώστε να μη μπορούν να υποστούν ζημιά.
- Κατά την διάρκεια μιας καταιγίδας ούτε να συνδέετε ούτε να βγάζετε τα καλώδια μεταφοράς δεδομένων, ούτε να τα ακουμπάτε.

Προβλεπόμενη χρήση, λειτουργία

- Το **X4100/200/300** προορίζεται για χρήση σε περιβάλλον γραφείου. Σαν Router πολλαπλών πρωτοκόλλων (Multi-Protokoll) το **X4100/200/**

300 σε εξάρτηση από την διαμόρφωση του συστήματος δημιουργεί συνδέσεις WAN. Για να αποφύγετε πρόσθετα τέλη θα πρέπει οπωσδήποτε να επιτηρείτε την συσκευή.

- Το **X4100/200/300** ανταποκρίνεται στις σχετικές διατάξεις ασφαλείας για εγκαταστάσεις τεχνολογίας πληροφοριών κατά τη χρήση σε περιβάλλον γραφείου.
- Η καθορισμένη λειτουργία του συστήματος σύμφωνα με το IEC950/EN60950 διασφαλίζεται μόνο με εγκαταστημένο περικάλυμμα (ψύξη, ασφάλεια πυρκαγιάς, εξάλειψη παρασίτων).
- Η θερμοκρασία περιβάλλοντος δεν επιτρέπεται 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.
- Το **X4100/200/300** δεν περιλαμβάνει εξαρτήματα που μπορούν να αντικατασταθούν από τον χρήστη ούτε διακόπτες ή Jumper, που πρέπει να ρυθμίσει ο χρήστης.
- Σε έκτακτες περιπτώσεις (π.χ. όταν έχει προκληθεί βλάβη στο κέλυφος ή στη μονάδα χειρισμού ή όταν έχουν εισέλθει υγρά ή αντικείμενα) να διακόπτετε αμέσως την παροχή ρεύματος και να έρχεστε σε επαφή με το κατάλληλο συνεργείο.

Καθαρισμός και επισκευή

- Η συσκευή επιτρέπεται να ανοιχτεί μόνον από συνεργεία που έχουν εξουσιοδοτηθεί από την BinTec. Πριν το άνοιγμα της συσκευής θα πρέπει οπωσδήποτε να βγάλετε τον ρευματολήπτη. Αναρμόδιο άνοιγμα και λανθασμένη επισκευή της συσκευής προκαλεί μεγάλο κίνδυνο για τον χρήστη (Ηλεκτροπληξία). Συνιστάται η επισκευή της συσκευής να γίνεται μόνο στο σέρβις του BinTec. Που υπάρχει σέρβις κοντά σας το μαθαίνετε απο τον έμπορο σας. Σε κάθε άλλη περίπτωση χάνεται κάθε δικαίωμα αξίωσης αποζημιώσεων.
- 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 συρμάτινα σφουγγαράκια 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 Router.

Trasporto e immagazzinaggio

- Trasportare ed immagazzinare **X4100/200/300** soltanto nell'imballaggio originale o in altro imballaggio adeguato a garantire protezione da urti e colpi.

Installazione e azionamento

- Prima di installare ed usare **X4100/200/300** fare attenzione alle istruzioni sulle condizioni ambientali (cfr. Dati tecnici). Utilizzare un ripiano stabile e piano.
- Le cariche elettrostatiche possono provocare danni all'apparecchio. Indossare quindi un polsino elettrostatico o toccare una superficie collegata a terra prima di afferrare prese o schede di espansione di **X4100/200/300**. Tenere sempre le schede di espansione soltanto per i bordi e non toccare gli elementi costruttivi né le guide per i conduttori.
- Proteggere lo slot per la scheda di espansione non utilizzato con la copertura, per evitare che penetrino oggetti nell'apparecchio. Se nell'apparecchio ci sono corpi estranei durante il funzionamento, sussiste pericolo di scosse elettriche e di corto circuito.
- Fare in modo che nessun oggetto appuntito possa danneggiare la finestra del modulo di visualizzazione. Proteggere il modulo di visualizzazione da urti e cadute e collegarlo soltanto all'apposito attacco RJ11 di **X4100/200/300**, per evitare danni a **X4100/200/300** e al modulo stesso.
- Durante il collegamento dei cavi occorre accertarsi che le fessure di ventilazione dell'apparecchio non vengano coperte e che la ventilazione non sia ostacolata. L'impedimento della ventilazione di **X4100/200/300** può danneggiare l'apparecchio. Danni provocati dalla carenza di ventilazione causano la perdita del diritto di garanzia.
- Non aprire l'apparecchio base e non effettuare alcuna modifica sull'alimentatore, poiché sussiste pericolo di morte causata da scosse elettriche. Non rimuovere le viti di fissaggio dell'apparecchio base.
- Quando l'apparecchio viene trasferito da un ambiente freddo nel locale di esercizio, l'involucro esterno e l'interno dell'apparecchio possono presen-

tare tracce di condensazione. Attendere finché l'apparecchio ha superato lo sbalzo di temperatura ed è assolutamente asciutto, prima di metterlo in funzione. Attenersi alle condizioni ambientali riportate nei dati tecnici

- Verificare se la tensione di rete locale corrisponde alle tensioni nominali dell'alimentatore. L'apparecchio deve essere impiegato alle seguenti condizioni:
  - 100 - 240 V c. a.
  - 50/60 Hz
- Accertarsi che la presa con contatto di terra dell'installazione sia accessibile. Per la completa separazione dell'apparecchio dalla rete di alimentazione è necessario estrarre la spina.
- Per il cablaggio si deve seguire la sequenza descritta nel manuale. Utilizzare soltanto i cavi rispondenti alle specifiche riportate in questo manuale o quelli originali forniti in dotazione. Se si utilizzano altri cavi, la BinTec Access Networks GmbH non risponde dei danni o della riduzione di funzionalità che ne risultano. In questi casi decade la garanzia per l'apparecchio.
- Per il collegamento dell'apparecchio ci si deve attenere alle istruzioni del manuale.
- Disporre i collegamenti in modo che non costituiscano fonte di pericolo (pericolo d'inciampo) e che non possano essere danneggiati.
- Non collegare né disconnettere, né toccare i cavi di trasferimento dati durante un temporale.

Utilizzazione conforme alla destinazione, funzionamento

- **X4100/200/300** è concepito per l'impiego negli uffici. Come Router per reti multiprotocollo **X4100/200/300** stabilisce collegamenti WAN in rapporto alla configurazione del sistema. Per evitare canoni indesiderati, si consiglia di controllare assolutamente il prodotto.
- **X4100/200/300** è conforme alle relative disposizioni di sicurezza per impianti della tecnica informatica impiegati in ambiente d'ufficio.
- Il funzionamento regolamentare del sistema secondo le disposizioni IEC 950/EN 60950 è garantito (raffreddamento, protezione antincendio, schermatura contro radiodisturbi) solo se è completamente montato l'involucro di lamiera.

- La temperatura ambiente non deve superare 50 °C. Non esporre l'apparecchio all'azione diretta dei raggi solari.
- Fare attenzione che nessun oggetto (p. es. fermagli) o liquido penetri all'interno dell'apparecchio (scossa elettrica, corto circuito). Provvedere ad un sufficiente raffreddamento.
- **X4100/200/300** non contiene elementi costruttivi che possono essere sostituiti dall'utente né interruttori/ponticelli che devono essere regolati dal cliente.
- In casi d'emergenza (p. es. danneggiamento dell'involucro o dell'elemento di comando, infiltrazione di liquido o di corpi estranei) staccare immediatamente la corrente ed informare il servizio assistenza.

Pulizia e riparazione

- L'apparecchio deve essere aperto soltanto da un centro di assistenza BinTec autorizzato. Prima di aprire l'apparecchio estrarre assolutamente la spina di alimentazione. L'apertura da parte di personale non autorizzato e riparazioni non corrette possono esporre l'utilizzatore a notevoli pericoli (p. e. scossa elettrica). Affidare l'esecuzione delle riparazioni all'apparecchio soltanto ad un centro di assistenza BinTec autorizzato. Il rivenditore di fiducia può fornire informazioni sulle sedi di questi centri. In tutti gli altri casi decade ogni diritto alla garanzia.
- 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 utilizzare in nessun caso abrasivi, detergenti a base alcalina, attrezzatura affilata o abrasiva.

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

- Transporteer en bewaar **X4100/200/300** 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 **X4100/200/300** op de instructies voor de omgevingsvoorwaarden (vergelijk technische gegevens). Gebruik een harde en vlakke ondergrond.
- Elektrostatische opladingen kunnen schade aan het toestel veroorzaken. Draag daarom een geaarde manchet rond de pols of raak een geaard oppervlak aan vooraleer u de bussen of uitbreidingskaarten van **X4100/200/300** aanraakt. Raak de uitbreidingskaarten enkel aan de randen aan en neem geen componenten of conductoren vast.
- De uitbreidingsslots die niet gebruikt worden met de blinde afdekking gesloten houden, zodat er geen voorwerpen in het inwendige deel van het toestel terecht kunnen komen. Als er zich tijdens het gebruik vreemde voorwerpen in het toestel bevinden, dan bestaat er gevaar voor stroomstoten en kortsluiting.
- Zorg ervoor dat het displayvenster van de displaymodule niet door scherpe voorwerpen beschadigd wordt. Beveilig de displaymodule tegen het stoten en vallen en sluit de module enkel aan de daarvoor bestemde RJ11-bus van **X4100/200/300** aan om schade aan de **X4100/200/300** en de displaymodule te vermijden.
- Zorg er bij de bedrading voor dat de ventilatie-openingen van het toestel niet afgedekt worden en de ventilatie niet gehinderd wordt. Door het hinderen van de ventilatie van de **X4100/200/300** kan het toestel beschadigd worden. We kunnen geen garantie geven voor schade die veroorzaakt werd door een gebrekkige ventilatie.
- Het basistoestel nooit openen en nooit manipuleren aan het netdeel omdat er anders gevaar voor stroomstoten bestaat. Geen schroeven van de bevestiging van het basistoestel verwijderen.

- Als het toestel vanuit een koude omgeving in de bedrijfsruimte gebracht wordt, kan er aan de buiten- en binnenkant van het toestel condensatie optreden. Wacht tot uw toestel zich aan de temperatuur heeft aangepast en helemaal droog is vooraleer u het in gebruik neemt. Neem de milieuvoorschriften in de technische gegevens in acht.
- Ga na of de plaatselijke netspanning overeenstemt met de nominale spanningen van het netdeel. Het toestel mag onder de volgende voorwaarden gebruikt worden:
  – 100 - 240 VAC
  – 50/60 Hz
- Zorg ervoor dat de veiligheidscontactdoos van de installatie vrij toegankelijk is. Om het toestel helemaal van het net te scheiden moet de netstekker uitgetrokken worden.
- Let bij de aansluiting van de kabels op de volgorde, zoals in het handboek wordt beschreven. Gebruik enkel kabels die aan de specificaties in dit handboek voldoen of die meegeleverd werden. Indien u andere kabels gebruikt, is BinTec Access Networks GmbH niet aansprakelijk voor mogelijke schade of het slecht functioneren van het toestel. In dit geval vervalt de garantie.
- Bij de aansluiting van het toestel de voorschriften in de handleiding in acht nemen.
- Leg de kabels zodanig, dat zij geen gevaarsbron (struikelgevaar) vormen en niet worden beschadigd.
- Tijdens een onweer de datatransmissielijnen niet aansluiten, uittrekken of aanraken.

Doelmatig gebruik, bedrijf

- **X4100/200/300** is enkel voor het gebruik in een bureau-omgeving geschikt. Als multi-protocol-router bouwt **X4100/200/300** afhankelijk van de systeemconfiguratie WAN-verbindingen op. Om ongewenste kosten te vermijden, moet het product absoluut gecontroleerd worden.
- **X4100/200/300** voldoet aan de gebruikelijke veiligheidsbepalingen voor inrichtingen van informatietechniek voor toepassing in een kantooromgeving.

- De reglementaire werking volgens IEC950/EN60950 van het systeem is alleen gegarandeerd bij een volledig gemonteerde blikken omhulling (koeling, brandbeveiliging, ontstoring.
- De omgevingstemperatuur mag niet hoger zijn dan 50 °C. Vermijd direct zonlicht.
- Let erop, dat er geen voorwerpen (bijv. paperclips) of vloeistoffen in het inwendige van het apparaat geraken (elektrische schok, kortsluiting). Let op voldoende koeling.
- **X4100/200/300** bevat geen modules die door de gebruiker vervangen mogen worden of schakelaars/jumpers die de gebruiker moet instellen.
- Onderbreek 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 toestel mag alleen door een door BinTec geautoriseerde servicedienst geopend worden. Voor het openen van het toestel in elk geval de netstekker uittrekken. Door onbevoegd openen en ondeskundige reparaties kan er groot gevaar voor de gebruiker ontstaan. (b. v. stroomstoten). Reparaties aan het toestel enkel door een door BinTec geautoriseerde servicedienst laten uitvoeren. Waar zich deze servicedienst bevindt, weet uw handelaar. In alle andere gevallen vervalt de aanspraak op garantie.
- 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.
- Gebruik 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 **X4100/200/300** i originalemballasjen eller i en annen egnet emballasje som beskytter mot støt og slag.

Oppstilling og ibruktaking

- Før oppstilling og drift av **X4100/200/300** må du ta hensyn til henvisningene når det gjelder omgivelsesbetingelsene (sml. tekniske data). Bruk et fast og jevnt underlag.
- Elektrostatisk oppladning kan føre til skader på apparatet. Bruk derfor en jordet mansjett rundt håndleddet eller berør en jordet flate før du berører kontakter eller utvidelseskort på **X4100/200/300**. Utvidelseskortene skal prinsipielt kun gripes i kantene, ta ikke på komponenter eller lederbaner.
- Hold utvidelses-stikkplassene som ikke er i bruk stengt med blinddekselet, slik at ingen gjenstander kan komme inn i apparatets indre. Hvis det finnes uvedkommende gjenstander i apparatet under drift, er det fare for elektrisk støt og kortslutning.
- Pass på at ikke spisse gjenstander forårsaker skader på displaymodulens displayvindu. Utsett ikke displaymodulen for støt eller fall, og kople den kun til den hertil tiltenkte RJ11-kontakt på **X4100/200/300**, slik at du unngår skader på **X4100/200/300** og displaymodulen.
- Under tilkoplingen må du passe på at apparatets ventilasjonsåpninger ikke blir tildekket og at ventilasjonen ikke blir hindret. Ved nedsatt ventilasjon av **X4100/200/300** kan det oppstå skader på apparatet. Skader som oppstår på grunn av manglende ventilasjon fører til tap av garantien.
- Åpne ikke basisapparatet og utfør ingen manipulasjoner på nettdelen, ettersom det i så fall er livsfare på grunn av elektrisk støt. Fjern ingen festeskruer på basisapparatet.
- Dersom 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 routeren har tilpasset seg temperaturen og er helt tørr før du tar den i bruk.

- Kontroller at nettspenningen på stedet er identisk med nettdelens merkespenning. Apparatet kan tas i drift under følgende betingelser:
  – 100 - 240 VAC
  – 50/60 Hz
- Kontroller at det er fri tilgang til installasjonens jordete stikkontakt. Nettstøpselet må trekkes ut for at apparatet skal være fullstendig frakoplet nettet.
- Følg den rekkefølgen som er beskrevet i håndboken under tilkopling. Bruk kun kabler som svarer til spesifikasjonene i denne håndboken eller som fulgte med i original i leveringen. Hvis du bruker andre kabler, påtar seg BinTec Access Networks GmbH intet ansvar for eventuelle skader eller nedsatt funksjonalitet. Garantien på apparatet oppheves i slike tilfeller.
- Følg instruksene i håndboken under tilkoplingen av apparatet.
- Legg opp ledningene slik at de ikke kan bli skadet og at de ikke danner farekilder (fare for å snuble).
- I tordenvær må du verken tilkople dataoverføringsledningene eller frakople eller berøre dem.

Forskriftsmessig bruk, drift

- **X4100/200/300** er beregnet på bruk i et kontorlandskap. I egenskap av multi-protokoll-router bygger **X4100/200/300** opp WAN-forbindelser, avhengig av systemkonfigurasjonen. Det er tvingende nødvendig å overvåke produktet for å unngå utilsiktede gebyrer..
- **X4100/200/300** oppfyller gjeldende sikkerhetsbestemmelser for innretninger innen informasjonsteknikk for bruk i kontorlanskapp.
- Forskriftsmessig bruk IEC950/EN60950 av systemet er kun gitt ved komplett montert metalldeksel (kjøling, brannbeskyttelse, radio-støydempning).
- Omgivelsestemperaturen må ikke overskride 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.
- **X4100/200/300** inneholder ingen komponenter som kan byttes ut av brukeren, eller brytere/jumpere som brukeren må innstille.

- I nødstilfeller (f.eks. skadet hus eller betjenings-elementer, når væske eller fremmedlegemer er kommet inn) må du straks bryte strømforsyningen og tilkalle service.

Rengjøring og reparasjon

- Apparatet skal kun åpnes av et BinTec-autorisert serviceverksted. Trekk ut nettstøpselet før apparatet åpnes. Ved uautorisert åpning og usakkyndige reparasjoner kan det oppstå alvorlige risikoer for brukeren (f. eks. fare for elektrisk støt). Se til at reparasjoner på apparatet kun utføres av et BinTec-autorisert serviceverksted. Din forhandler kan fortelle deg hvor nærmeste serviceverksted er. I alle andre tilfeller tapes garantien.
- Apparatet må under ingen omstendighet rengjøres med vann. Dersom vann trenger inn, kan det oppstå alvorlige risikoer for brukeren (f. eks. elektrisk støt) og alvorlige skader på apparatet.
- Bruk aldri skuremidler, alkaliske rengjøringsmidler, skarpe eller skurende hjelpemidler.

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 **X4100/200/300** 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 **X4100/200/300** tenha em conta as indicações relativas às condições ambientais (cf. Dados técnicos). Utilize uma base consistente e lisa.
- As cargas electrostáticas podem causar danos nos aparelhos. Por conseguinte, use um punho de ligação terra à volta do pulso ou então toque numa superfície ligada à terra antes de mexer nas tomadas ou placas de expansão do **X4100/200/300** . Toque apenas nos bordos das placas de expansão e não toque nos componentes ou circuitos impressos.
- Mantenha a slot de expansão não utilizada fechada com a cobertura cega, de modo a que não possa entrar qualquer objecto no interior do aparelho. Se, durante o funcionamento, houver algum objecto estranho dentro do aparelho, existe perigo de choque eléctrico e de curto-circuito.
- Tenha cuidado para que nenhum objecto pontiagudo danifique a janela do módulo de display. Para evitar danos no **X4100/200/300** e no módulo de display, proteja o módulo de display contra embates fortes e quedas e conecte o mesmo à tomada RJ11 do **X4100/200/300** destinada a esse fim.
- Durante a cablagem, tenha atenção para que as ranhuras de ventilação do aparelho não fiquem tapadas e a ventilação não seja obstruída. A obstrução da ventilação do **X4100/200/300** pode causar danos no aparelho. Os danos causados por uma ventilação insuficiente têm como consequência a perda da garantia.
- Não abra o aparelho base, nem mexa no equipamento de alimentação de rede, uma vez que existe perigo de morte devido a choque eléctrico. Não retire quaisquer parafusos de fixação do aparelho base.
- Quando o aparelho é deslocado de um local frio para o local de funcionamento, poderá haver formação de condensação tanto no exterior como no

interior do aparelho. Aguarde até o aparelho se encontrar à temperatura ambiente e completamente seco antes de o colocar em funcionamento. Tenha em atenção as indicações relativas às condições ambientais nos Dados técnicos.

- Verifique se a tensão de rede local corresponde às tensões nominais do equipamento de alimentação de rede. O aparelho pode ser operado nas seguintes condições:
  – 100 - 240 VAC
  – 50/60 Hz
- Certifique-se de que a tomada de contacto de segurança da instalação está acessível. Para desligar completamente a corrente do aparelho, retire a ficha de rede.
- Ao proceder à cablagem, respeite a sequência tal como está descrita no manual. Utilize unicamente cabos que correspondam às especificações contidas neste manual ou cabos originais que tenham sido fornecidos. Se usar outros cabos, a BinTec Access Networks GmbH não se responsabiliza por danos daí decorrentes ou por limitações de funcionamento. Nestes casos, a garantia do aparelho é anulada.
- Aquando da conexão do aparelho, respeite as indicações constante do manual.
- Instale os cabos de maneira a não constituírem uma fonte de perigo (perigo de tropeçar) nem se danificarem.
- Em caso de trovoada, não ligue, retire ou toque nos cabos de transmissão de dados.

Utilização conforme com as especificações, Operação

- O **X4100/200/300** destina-se à utilização em escritórios. Como Router de protocolos múltiplos, o **X4100/200/300** constrói ligações WAN de acordo com a configuração do sistema. Para evitar custos indesejados, controle o produto.
- O **X4100/200/300** corresponde às normas de segurança habituais relativas a dispositivos de informática para utilização em escritórios.
- Só é possível assegurar o funcionamento adequado do sistema em conformidade com IEC950/EN60950 se a caixa de chapa estiver completamente

montada (refrigeração, protecção contra incêndio, supressão de interferências).

- A temperatura ambiente não pode exceder os 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.
- O **X4100/200/300** não contém componentes que possam ser substituídos pelo utilizador ou interruptores/conectores que o utilizador tenha de regular.
- 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 num serviço de assistência técnica BinTec autorizado. Antes de abrir o aparelho é indispensável retirar a ficha de rede. A abertura não autorizada e as reparações inadequadas podem representar riscos graves para o utilizador (por ex. choque eléctrico). Mande efectuar as reparações do aparelho apenas nos serviços de assistência técnica BinTec autorizados. O seu fornecedor indicar-lhe-á a localização dos referidos serviços. Caso contrário, perderá todos os direitos de garantia.
- 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 **X4100/200/300** 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 **X4100/200/300**, observe las instrucciones acerca de las condiciones ambientales (ver Datos técnicos). Utilice una superficie firme y plana.
- Las cargas electrostáticas pueden ocasionar daños en los aparatos. Por ello, lleve un puño puesto a tierra alrededor de la muñeca o entre en contacto con una superficie puesta a tierra antes de tocar hembrillas o tarjetas de expansión de **X4100/200/300**. Toque las tarjetas de expansión sólo en los bordes y no entre en contacto con componentes ni con redes de circuitos impresos.
- Mantenga cerrada la ranura de expansión con la cubierta ciega para que no pueda penetrar ningún objeto en el interior del aparato. Si durante el servicio hubiera dentro algún objeto extraño, se correría peligro de electrocución y de cortocircuito.
- Preste atención a que ningún objeto afilado dañe la ventana de display del módulo de display. Proteja este módulo frente a golpes y caída y conéctelo únicamente a la hembrilla RJ11 prevista en **X4100/200/300** a fin de evitar daños en **X4100/200/300** y en el módulo de display.
- Al instalar los cables, preste atención a no cubrir las rendijas de ventilación del aparato para no impedir la ventilación. Si la ventilación de **X4100/200/300** resultase afectada, podrían ocasionar daños en el aparato. Los daños producidos a causa de una ventilación insuficiente conllevan la pérdida de garantía.
- No abra el aparato base, ni manipule de ningún modo el bloque de alimentación, ya que en caso contrario se corre peligro de muerte por electrocución. No retire ninguno de los tornillos de fijación del aparato base.

- Si el aparato proviene de un ambiente frío, al introducirlo en el local de trabajo se puede producir deshielo tanto en su exterior como en su interior. Por ello, antes de ponerlo en funcionamiento espere a que su temperatura se haya igualado y a que esté totalmente seco. Preste atención a las condiciones medioambientales expuestas en el apartado de Datos Técnicos.
- Asegúrese de que la tensión de la red local coincida con las tensiones nominales del bloque de alimentación. El aparato puede funcionar bajo las siguientes condiciones:
  - 100 - 240 VCA
  - 50/60 Hz
- Asegúrese de que no quede obstaculizado el acceso a la caja de enchufe con puesta a tierra de la instalación. Para desconectar totalmente el aparato de la red es necesario desenchufar el enchufe de la red.
- Al instalar los cables respete el orden descrito en el manual. Utilice únicamente cables que cumplan las especificaciones expuestas en este manual o que hayan venido incluidos en el volumen de suministro. Si utiliza otros cables, BinTec Access Networks GmbH no se hará responsable en el caso de que se produzcan daños o una merma en el funcionamiento. En estos casos la garantía pierde su validez.
- Al conectar el aparato, respete las indicaciones dadas en el manual.
- Coloque los cables de manera que no constituyan un peligro (tropezones) y no puedan ser deteriorados.
- Durante una tormenta, no enchufe ni desenchufe los conductos de transmisión de datos, ni los toque.

Utilización prevista, servicio

- **X4100/200/300** está concebido para ser utilizado en oficinas. Como router multiprotocolo, **X4100/200/300** establece conexiones WAN dependiendo de la configuración del sistema. Para evitar que se produzcan gastos de conexiones indeseadas, es absolutamente necesario vigilar el producto.
- **X4100/200/300** corresponde a las disposiciones de seguridad pertinentes para equipos informáticos utilizados en oficinas y despachos.

- El servicio correspondiente al destino según IEC 950/EN 60950 del sistema está sólo asegurado al estar montada completamente la caja de chapa (refrigeración, protección contra incendios, antiparasitaje).
- La temperatura ambiente no debe ser superior a los 50 °C. Evite que el aparato quede expuesto 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.
- El usuario de **X4100/200/300** no puede cambiar ningún componente, ni debe ajustar ningún interruptor/puente.
- 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

- Sólo personal de un servicio técnico autorizado por Bin Tec puede abrir el aparato. Antes de abrirlo, es imprescindible desconectar el enchufe de la red. Si se abre de forma no autorizada o las reparaciones no se efectúan como es debido, esto puede suponer riesgos considerables para el usuario (p. ej., electrocución). Por ello, encargue siempre los trabajos de reparación a un servicio técnico autorizado por BinTec, cuya dirección se la proporcionará su distribuidor. De otro modo, perderá todo el derecho de garantía.
- 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 svenska

Beakta alltid nedanstående säkerhetsanvisningar för användning av apparaten.

Transport och förvaring

- **X4100/200/300** får endast transporteras och förvaras i originalförpackningen eller i en annan likvärdig förpackning som ger ett fullvärdigt skydd mot stötar och slag.

Installation och start

- Beakta uppgifterna om omgivningsförhållanden (se Tekniska data) innan **X4100/200/300** installeras och startas. Installera den på ett stabilt och jämnt underlag.
- Elektrostatisk uppladdning kan förorsaka skador på apparaten. Bär därför en antistatisk manschett runt handleden, eller rör alltid vid en jordad yta innan Du vidrör uttag/kontakter eller utbyggnadskort till **X4100/200/300**. Tag endast på utbyggnadskortens kanter, vidrör aldrig ledningarna och komponenterna.
- Täck över en ej använd utbyggnadsinsticksplats med täckskivan så att inga främmande föremål kan komma in i apparaten. Risk för strömstötar och kortslutning om främmande föremål finns i apparaten under drift.
- Säkerställ att displaymodulens displayfönster inte kan skadas av några spetsiga föremål. Installera displaymodulen så att den inte kan falla ned resp utsättas för stötar och slag. Anslut den endast till härför avsett RJ11-uttag **X4100/200/300** , annars kan **X4100/200/300** och displaymodulen ta skada.
- Säkerställ, under kabeldragningen, att apparatens ventilationsslitsar inte täcks över och att ventilationen inte påverkas. En reducerad ventilationseffekt kan medföra skador på **X4100/200/300**. Tillverkaren övertar inget garantiansvar för skador som uppstår p g a bristfällig ventilation.
- Öppna inte basenheten, utför inga som helst förändringar på nätdelen; risk för strömstötar, livsfara. Tag inte bort några montageskruvar från basenheten.
- Om enheten flyttas från en kall till en varm omgivning kan det bildas kondensvatten på och i apparaten. Tag apparaten i drift först när den har nått rumstemperatur och har torkat helt. Beakta uppgifterna över omgivningsförhållanden i Tekniska data.

- Kontrollera att spänningen på plats överensstämmer med nätdelens märkspänning. Under följande villkor får apparaten användas:
  – 100 - 240 VAC
  – 50/60 Hz
- Säkerställ att det jordade vägguttaget alltid är fritt tillgängligt. För separering från nätet måste nätkontakten dras ut.
- Utför kabeldragningen i den ordningsföljd som anges i handboken. Använd endast medlevererade originalkablar eller kablar som överensstämmer med specifikationerna i denna handbok. BinTec Access Networks GmbH påtar sig inget ansvar för eventuella skador eller brister på apparaten om den används tillsammans med andra kablar. I detta fall gäller inte garantin längre.
- Beakta anvisningarna i handboken vid anslutning av apparaten.
- Drag kablarna så att de inte kan utgöra någon fara (de får inte ligga så att man kan snubbla över dem) och så att de inte kan skadas.
- Dataöverföringskabeln får inte anslutas, dras ut eller vidröras under ett åskväder.

Ändamålsenlig användning, drift

- **X4100/200/300** är avsedd för användning i kontorslokaler. **X4100/200/300** är en multi-protokoll-router som, beroende på systemkonfiguration, upprättar WAN-förbindelser. Produkten bör övervakas så att inte onödiga kostnader uppstår.
- **X4100/200/300** uppfyller kraven i alla relevanta säkerhetsbestämmelser för informationsteknikutrustning i kontorslokaler.
- Ändamålsenlig användning av systemet enligt IEC 950/EN 60950 säkerställs endast om plåthöljet är komplett monterat (kylning, brandskydd, radioavstörning).
- Omgivningstemperaturen bör inte vara högre än 50°C . Undvik direkt solljus.
- Säkerställ att det inte kan komma in några föremål (t ex häftklammer) eller någon vätska i apparaten (strömstötar, kortslutning). Sörj för fullgod kylning.

- **X4100/200/300** har inga komponenter som användaren kan byta ut, och inga kontakter/jumpers som måste ställas in.
- Koppla genast ifrån strömförsörjningen i nödsituationer (t ex skadat hölje eller skadade manöverelement, eller om vätska eller främmande föremål har kommit in i apparaten) och tag kontakt med serviceavdelningen.

Rengöring och reparation:

- Apparaten får endast öppnas av en av BinTEc auktoriserad serviceverkstad. Drag alltid ut nätkontakten innan apparaten öppnas. Obehörigt öppnande resp ej sakkunniga reparationer på apparaten kan medföra fara för användaren (t ex elektriska stötar). Reparationer får bara utföras av en av BinTec auktoriserad serviceverkstad. Återförsäljaren tillhandahåller information om närmaste serviceverkstad. I annat fall upphör garantiansvaret att gälla.
- Apparaten får aldrig våtrengöras. Vatten som kommer i enheten kan medföra fara för användaren (t ex elektriska stötar) och förorsaka skador på apparaten.
- Använd inget skurpulver, inga alkaliska rengöringsmedel, använd inga vassa resp repande hjälpmedel.

Genel güvenlik bilgileri türkçe

Müteakip bölümlerde cihazınızı kullanırken mutlaka dikkat etmeniz gereken genel güvenlik bilgilerini bulabilirsiniz.

Taşıma ve Depolama

- **X4100/200/300** cihazı sadece orjinal ambalajı içinde veya çarpmaya ve darbeye karşı koruyan uygun başka bir ambalajla taşıyıp depolayınız.

Kurulması ve Çalıştırılması

- **X4100/200/300** cihazını kurup çalıştırmadan önce çevre koşulları hakkındaki bilgileri dikkate alınız (bak. Teknik Bilgiler). Sağlam ve düz bir altlık kullanınız.
- Elektrostatik yüklenmeler cihazın zarar görmesine neden olabilir. Bu yüzden el bileğinize antistatik bir manşet takınız veya **X4100/200/300** cihazının soketleri ve modüllerine dokunmadan önce, topraklı bir yüzeye dokununuz. Modülleri yalnız kenarlarından tutunuz, yapı parçalarına veya hatlara dokunmayınız.
- Cihazın içine yabancı cisimlerin girmesini engellemek için kullanılamayan modül soketlerini körtapalarla kapatınız. Kullanım esnasında cihazın içinde yabancı cisimler bulunuyorsa, elektrik çarpması ve elektrik bağlantılarının kısa devre yapma tehlikesi bulunmaktadır.
- Sivri aletlerin display modülünün display penceresine zarar vermemesine dikkat ediniz. Display modülünü çarpma ve düşmeden koruyunuz ayrıca **X4100/200/300** cihazına ve display modülüne zarar gelmemesi için, sadece bunun için ön görülmüs olan **X4100/200/300** cihazının RTJ11 soketine bağlayınız.
- Kabloları yerleştirirken, cihazın havalandırma deliklerinin kapanmamasına ve havalandırmanın engellenmemesine dikkat ediniz. **X4100/200/300** cihazının havalandırması engellendiği takdirde cihaza zarar gelebilir. Yetersiz havalandırmanın yol açtığı zararlar, cihazın garanti hakkının kaybına sebeb verir.
- Ana cihazı kesinlikle açmayınız ve elektrik çarpması sonucunda hayati tehlike bulunduğundan, elektrik kablosunda hiçbir işlem yapmayınız. Ana cihazdan tespit vidalarını sökmeyiniz.
- Cihaz, çalıştırılacağı odaya soğuk bir ortamdan getirilmiş ise, cihazın dışında ve içinde çiylenme olabilir. Cihazınızı çalıştırmadan önce

tamamen kurumasını ve oda sıcaklığına uyum sağlamasını bekleyiniz. Teknik Bilgiler'deki çevre koşullarını dikkate alınız.

- Yerel şebeke geriliminin, şebeke parçasının nominal gerilimine uygun olup olmadığını kontrol ediniz. Cihaz, aşağıdaki koşullar doğrultusunda çalıştırılabilir:
  - 100 - 240 VAC
  - 50/60 Hz
- Koruyucu kontak prizinin montaj için rahatlıkla ulaşılabilecek durumda olmasını sağlayınız. Şebekeden tamam kopmak için, elektrik fişinin prizden çekilmeşi gerekir.
- Kabloları takarken el kitapcığındaki sıralamaya dikkat ediniz. Sadece el kitapcığında belirtilen verilere uygun veya cihazla birlikte gönderilen kabloları kullanınız. Başka kablo kullandığınız takdirde, BinTec Access Networks GmbH meydana gelen hasar veya fonksiyonlardaki olumsuz etkilerden dolayı sorumluluk üstlenmez. Bu durumlarda garanti hakkı ortadan kalkar.
- Cihazı bağlarken el kitapcığındaki açıklamalara dikkat ediniz.
- Kabloları, tehlike kaynağı olamayacak ve zarar görmeyecek şekilde (takılma tehlikesi) döşeyiniz.
- Fırtına esnasında veri iletişim hatlarını ne bağlayınız, ne çıkartınız, ne de bunlara dokununuz.

Belirlenmiş şekilde kullanım, işletim

- **X4100/200/300** cihazı büro ortamında kullanım için tasarlanmıştır. Multi-Protokol-Router olarak **X4100/200/300** cihazı sistem konfigurasyonuna bağlı olarak WAN-bağlantıları kurmaktadır. Istenmeyen masrafları önlemek için, ürünü mutlaka kontrol altında tutunuz.
- **X4100/200/300** cihazı, büro ortamında kullanılan enformasyon teknik donanımları için geçerli olan güvenlik talimatnamelerine kesinlikle uymaktadır.
- IEC 950/EN 60950 uyarınca, sistemin belirlenmiş şekilde kullanımı sadece saç kasnağı tamamiyle monte edildiğinde sağlanabilir (soğutma, yangın önleme, parazit giderme).

- Çevre sıcaklığı kesinlikle 50°C'yi geçmemeli. Cihazı direk gelen güneş ışınlarından koruyunuz.
- Cihazın içine yabancı cisimlerin (örneğin ataç) veya sıvıların girmesini önleyiniz (elektrik çarpması, kısa devre). Cihazın yeterli oranda soğutulmasına dikkat ediniz.
- **X4100/200/300** cihazında, kullanıcı tarafından değiştirilebilecek herhangi bir yapı elemanı veya kullanıcının ayarlaması gereken şalter/jumper bulunmamaktadır.
- Acil durumlarda (örneğin hasarlı cihaz kasası veya kullanım parçası, cihazın içine sıvı veya yabancı maddelerin girmesi) derhal elektrik akımını kesip servise haber veriniz.

Temizlik ve Tamir

- Cihaz sadece BinTec'in yetkili servisi tarafından açılabilir. Cihazı açmadan önce, mutlaka elektrik fişini prizden çekiniz. Müsaade edilen işlemler dışında açılması ve uygun olmayan şekilde tamir edilmesi, kullanıcı için büyük tehlikeler doğurabilir (örneğin elektrik çarpması). Cihazın tamiratını sadece BinTec yetkili servisi tarafından yaptırınız. Yetkili servis yerlerini nerede bulabileceğinizi satıcınızdan öğrenebilirsiniz. Diğer durumlarda garanti hakkı kaybolmaktadır.
- Cihazın su ile temizlenmesi kesinlikle yasaktır. Suyun cihaz içine kaçması, kullanıcı için büyük tehlikeler doğurabilir (örneğin elektrik çarpması) ve cihaza da ciddi zararlar verebilir.
- Kesinlikle temizleme tozları, alkalik temizlik maddeleri, keskin veya aşındırıcı yardımcı maddeler kullanmayınız.

Általános biztonsági útmutató

A következő fejezetekben olyan biztonsági útmutatásokat talál, amelyeket a készüléke alkalmazása során feltétlenül figyelembe kell vennie.

Szállítás és tárolás

- Az **X4100/200/300** csak az eredeti vagy egy más, arra alkalmas csomagolásban szállítandó és tárolandó, amely lökések és ütések ellen védelmet biztosít.

Felállítás és üzembe helyezés

- Az **X4100/200/300** felállítása és üzembe helyezése előtt vegye figyelembe a környezeti feltételekre vonatkozó utasításokat (v.ö. a műszaki adatokkal). A készüléket szilárd és sík alapon alkalmazza.
- Az elektrosztatikus töltések kisülése a berendezés meghibásodásához vezethet. Ezek megelőzése céljából viseljen földelt csuklópántot, vagy érintsen meg egy földelt felületet, mielőtt az **X4100/200/300** csatlakozóhüvelyeihez vagy bővítőkártyáihoz hozzáérne. A bővítőkártyákat mindig csak a szélükön érintse meg, sose érjen alkatrészekhez vagy vezető vonalakhoz.
- A nem használt slotokat mindig zárja le vakfedéllel, hogy ne kerülhessenek idegen tárgyak a készülék belsejébe. Amennyiben idegen tárgyak kerülnek a készülék belsejébe, áramütés és rövidzárlat veszélye áll fenn.
- Ügyeljen arra, hogy a displaymodul display-jét semmilyen hegyes tárgy ne sérthesse meg. Óvja a displaymodult lökésektől és leeséstől. A displaymodult csak az **X4100/200/300** erre kijelölt RJ11 csatlakozóhüvelyére csatlakoztassa, hogy az **X4100/200/300** készüléken és a displaymodulon emiatt keletkező meghibásodásokat elkerülje.
- A vezetékezésnél ügyeljen arra, hogy a készülék szellőzőnyílásai ne legyenek letakarva, a szellőzés zavartalanul működjék. A nem megfelelő szellőzés az **X4100/200/300** meghibásodásához vezethet. A nem megfelelő szellőzés miatt fellépő károk esetében garanciaigénye megszűnik.
- Ne nyissa ki a készülék burkolatát, és ne végezzen semmilyen átalakítást a tápegységen, mert ezáltal életveszélyes áramütés veszélye áll fenn. Ne távolítsa el a készülék rögzítő csavarjait.
- Ha a készülék hideg környezetből kerül az üzemeltetési helyére, akkor a készülék külsején és belsejében lecsapódhat a nedvesség. Az üzembe

helyezés előtt várja meg, amíg a készülék el nem éri a szobahőmérsékletet, és teljesen meg nem szárad. Vegye figyelembe a műszaki adatoknál megadott környezeti feltételeket.

- Ellenőrizze, hogy a helyi hálózati feszültség megegyezik-e a tápegység névleges feszültségével. A készülék az alábbi feltételek mellett üzemeltethető:
  – 100 - 240 VAC
  – 50/60 Hz
- Gondoskodjon róla, hogy a védőérintkezős csatlakozó aljzat a telepítésnél hozzáférhető legyen. A hálózatról való teljes leválasztáshoz húzza ki a hálózati csatlakozót.
- A vezetékezés során vegye figyelembe a kézikönyvben megadott sorrendet. Csak olyan vezetékeket alkalmazzon, amelyek a kézikönyvben megadott specifikációknak megfelelnek, vagy amelyek a készülék szállítási terjedelmében találhatók. Amennyiben más vezetékeket alkalmaz, az emiatt fellépő károkért vagy a működésben fellépő változásokért a BinTec Access Networks GmbH nem vállal felelősséget. Ebben az esetben megszűnik a garanciajogosultsága.
- Vegye figyelembe a készülék csatlakoztatásánál a kézikönyvben leírt ide vonatkozó utasításokat.
- A vezetékeket úgy fektesse le, hogy azok ne lehessenek veszélyek forrásai (botlásveszély), azokban pedig kár ne keletkezhessen.
- Az adatátvivő vezetékeket vihar esetében ne csatlakoztassa, ne húzza le, ne érintse meg.

Rendeltetésszerű alkalmazás, üzemeltetés

- Az **X4100/200/300** irodai környezetben való alkalmazásra készült. Az **X4100/200/300**, mint multi-protokoll-router, a rendszerkonfigurációtól függően a WAN-összeköttetésekre épül. A nem kívánt telefondíjak elkerülése végett, a terméket feltétlenül tartsa megfigyelés alatt.
- Az **X4100/200/300** megfelel az idevágó - irodai környezetben való használatra alkalmas információtechnikai berendezésekre vonatkozó - biztonsági előírásoknak.

- A rendszer rendeltetésszerű üzemeltetése az IEC 950/EN 60950 szabályzatnak megfelelően csak a teljesen összeszerelt fémburkolattal biztosítható (hűtés, tűzvédelem, zavarszűrés).
- A környezeti hőmérséklet nem haladhatja meg az 50 °C-t. Kerülje a közvetlen napsütést.
- Ügyeljen arra, hogy semmilyen tárgy (pl. gémkapocs) vagy folyadék ne kerülhessen a készülék belsejébe (áramütés, rövidzárlat). Ügyeljen a megfelelő hűtésre.
- Az **X4100/200/300** nem tartalmaz alkatrészeket, amelyeket a felhasználó kicserélhet, vagy kapcsolókat, jumpereket, amelyeket a felhasználónak kellene beállítania.
- Vészhelyzetben (pl. sérült burkolat vagy kezelőegység, folyadék vagy idegen test behatolása esetén) azonnal szakítsa meg az áramellátást, és értesítse a szervizt.

Tisztítás és javítás

- A készüléket csak a BinTec által feljogosított szervizek nyithatják fel. A készülék felnyitása előtt feltétlenül húzza ki a hálózati csatlakozót. A készülék jogtalan felnyitása és a helytelen javítás révén a felhasználó számára jelentős veszélyforrások keletkezhetnek (pl. áramütés). A készüléken szükséges javításokat ezért csak a BinTec által feljogosított szervizekkel végeztesse. A szervizek címét érdeklődje meg a szakkereskedőjénél. Ellenkező esetben a mindennemű garanciaigénye megszűnik.
- A készüléket semmi esetre sem szabad nedvesen tisztítani. A behatoló víz jelentős veszélyforrásokat jelenthet a felhasználó számára (pl. áramütés), és jelentős károkat okozhat a készüléken.
- Sohasem szabad súrolószereket, lúgos tisztítószereket, éles vagy karcoló segédeszközöket alkalmazni.

Všeobecné bezpečnostní pokyny

V následujících odstavcích jsou uvedeny bezpečnostní pokyny, které se při používání přístroje musí zásadně dodržovat.

Doprava a uskladnění

- **X4100/200/300** dopravujte a skladujte pouze v originálním obalu anebo v jiném vhodném obalu, který jej chrání proti nárazům.

Instalace a uvedení do provozu.

- Před instalací a provozem **X4100/200/300** přihlížejte k pokynům, které se týkají podmínek okolního prostředí (srovn. Technické údaje). Předpokládá se pevný a rovný podklad.
- Elektrostatické náboje mohou způsobit poškození přístroje. Použijte proto uzemněnou manžetu připevnenou kolem zápěstí anebo se nejprv dotkněte některé uzemněné plochy, než se budete dotýkat konektorových zásuvek nebo rozširujících desek **X4100/200/300**. Rozšiřovacích desek se zásadně dotýkejte pouze na okrajích a nesahejte na součásti nebo vodivé spoje.
- Uzavírejte nepoužívaný rozšiřovací slot záslepkou tak, aby do vnitřku přístroje nemohly vniknout cizí předměty. Pokud se během provozu v přístroji nacházejí cizí předměty, hrozí nebezpečí zasažení elektrickým proudem nebo zkratu.
- Dbejte na to, aby okno displeje u displejového modulu nebylo poškozeno ostrými, špičatými předměty. Chraňte displejový modul před poškozením nárazy a pádem a připojte jej pouze na příslušný konektor RJ11 u **X4100/200/300** , aby se zabránilo poškození **X4100/200/300** a displejového modulu.
- Při kabeláži dbejte na to, aby nedošlo k zakrytí větracích otvorů přístroje a aby nebyla omezována funkce větrání. V důsledku omezení větrání **X4100/200/300** by mohlo dojít k poškození přístroje. Škody vzniklé v důsledku nedostatečného větrání vedou ke ztrátě nároků z ručení.
- Neotevírejte základní přístroj a síťový zdroj nepodrobujte žádným manipulacím, jinak hrozí životní nebezpečí zasažením elektrickým proudem. Neodstraňujte žádné šrouby u upevnění základního přístroje.
- Pokud se přístroj přemístí z chladného prostředí do provozního prostoru, může se vyskytnout orosení jak na vnějších částech tak i uvnitř přístroje. Vyčkejte teplotní přizpůsobení přístroje a jeho absolutní vysušení, než jej uvedete

do provozu. Přihlížejte k podmínkám okolního prostředí uvedeným v Technických údajích.

- Kontrolujte, zda se napětí místní sítě shoduje s hodnotami jmenovitého napětí síťového zdroje. Přístroj lze provozovat za těchto podmínek:
  – 100 - 240 VAC
  – 50/60 Hz
- Postarejte se o to, aby zásuvka s ochranným kontaktem byla při instalaci volně přístupná. Pro úplné odpojení od sítě je třeba vytáhnout síťovou zástrčku.
- Při propojování dbejte na pořadí tak, jak je popsáno v příručce. Používejte pouze kabely, jež odpovídají specifikacím v této příručce anebo dodané originální kabely. Pokud použijete jiné kabely, odmítá BinTec Access Networks GmbH ručení za vzniklé škody nebo za omezenou funkčnost. Ručení za přístroj v těchto případech zaniká.
- Při připojování přístroje dbejte na pokyny uvedené v příručce.
- Vedení ukládejte tak, aby se nestala zdrojem nebezpečí (např. zakopnutím) a aby se nepoškodily.
- Během bouřky nepřipojujte vedení na přenos dat, neodpojujte je a ani se jich nedotýkejte.

Použití, provoz podle stanoveného účelu

- **X4100/200/300** je určen pro použití v kancelářském prostředí. Jako MultiProtocol Router sestavuje **X4100/200/300** v závislosti na systémové konfiguraci spojení WAN. Chcete-li zabránit účtování nežádoucích poplatků, měli byste výrobek bezpodmínečně hlídat.
- **X4100/200/300** odpovídá příslušným bezpečnostním předpisům pro zařízení informační techniky používaná v kancelářském prostředí.
- Provoz systému odpovídající stanovenému účelu podle IEC 950/EN 60950 je zaručen pouze při kompletní montáži plechového krytu (chlazení, protipožární ochrana, odrušení).
- Teplota okolí nesmí překročit 50 °C. Zabraňte přímému ozáření sluncem.

- Dbejte na to, aby do vnitřku přístroje nemohly vniknout žádné předměty (např. kancelářské svorky) anebo kapaliny (elektrický výboj, zkrat). Dbejte na dostatečné chlazení.
- **X4100/200/300** neobsahuje žádné součásti, které by uživatel směl vyměňovat, nebo spínače/propojky, které by uživatel musel nastavovat.
- V nouzových případech (např. poškozená skříň anebo ovládací prvek, vniknutí kapaliny nebo cizích těles) okamžitě přerušte přívod proudu a informujte servis.

Čištění aopravy

- Přístroj smí otvírat pouze autorizovaný servis firmy BinTec. Před otevřením se přístroj zásadně musí odpojit od sítě (vytáhnout zástrčku). Nepovolaným otevíráním a neodbornými opravami se uživatel vystavuje značnému ohrožení (např. zasažení elektrickým proudem). Provedením oprav přístroje pověřujte pouze autorizovaný servis firmy BinTec. Adresu servisu Vám sdělí Váš obchodník. Ve všech ostatních případech zanikají veškeré nároky ze záruky.
- Přístroj se zásadně nesmí čistit mokrým způsobem. Vnikající voda může uživatele vystavit značnému ohrožení (např. zasažení elektrickým proudem) a může způsobit značné poškození přístroje.
- Nikdy nepoužívejte prostředky na mechanické čištění, alkalické čisticí prostředky, agresivní a drhnoucí pomůcky.

Ogólne zasady bezpieczeństwa w jêzyku polskim

Poniżej podano zasady bezpieczeństwa, których należy bezwzględnie przestrzegać przy obchodzeniu się z routerem.

Transport i magazynowanie

- Urządzenie **X4100/200/300** 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 **X4100/200/300** należy zastosować się do wskazówek dotyczących warunków otoczenia (por. Parametry techniczne). Urządzenie należy ustawić na trwałym i równym podłożu.
- Elektrostatyczna różnica potencjałów może doprowadzić do uszkodzenia urządzenia. Przed przystąpieniem do pracy należy założyć na przegub ręki antyelektrostatyczną opaskę zabezpieczającą lub dotknąć uziemionej powierzchni zanim dojdzie do kontaktu dłoni z puszkami lub kartami rozszerzenia **X4100/200/300** Karty poszerzające chwytać zawsze na obrzeżach; nie dotykać bezpośrednio ścieżek drukowanych oraz elementów elektronicznych.
- Nie używane pole do dodatkowych wcisków zamknąć zaślepkami zabezpieczającymi które zapobiegają dostaniu się do wnętrza niepożądanych przedmiotów. Obecność obcych elementów w urządzeniu w czasie jego eksploatacji stanowi zagrożenie porażenia prądem lub prowadzi do spięcia elektrycznego.
- Zwrócić szczególną uwagę aby okienko displaya (pola wyświetlającego) w module displaya nie zostało uszkodzone ostrymi przedmiotami. Należy chronić moduł displaya przed uderzeniami i upadkiem i zamykać w do tego celu przeznaczonej puszce RJ11**X4100/200/300**, aby nie dopuścić do szkód na **X4100/200/300** i module displaya.
- Okablowanie powinno być tak prowadzone, żeby szczeliny wentylacyjne i otwory w obudowie nie zostały przysłonięte i w konsekwencji nie doszło do zakłócenia właściwego chłodzenia urządzenia. Niewystarczające przewietrzanie **X4100/200/300**może doprowadzić do awarii urządzenia. Uszkodzenia wynikające z niedostatecznej wentylacji mogą wiązać się z utratą reklamacji.

- Otwieranie urządzenia głównego i dokonywanie manipulacji w części przewodowej jest niedozwolone i grozi śmiertelnym porażeniem prądem. Zabronione jest odkręcanie śrub mocujących z urządzenia głównego.
- W momencie przemieszczenia urządzenia z zimnego otoczenia do pomieszczenia eksploatacyjnego, może wystąpić pokrycie parą zarówno części zewnętrznych jak i wewnętrznych. Należy odczekać aż urządzenie przejmie nową temperaturę i całkowicie wyschnie, dopiero wtedy możliwa jest jego eksploatacja. Należy przestrzegać warunków środowiskowych opisanych w danych technicznych urządzenia.
- Konieczne jest sprawdzenie zgodności napięcia sieci zasilającej z napięciem znamionowym zasilacza prądowego. Urządzenie może być eksploatowane pod następującymi warunkami:
  - 100 - 240 VAC
  - 50/60 Hz
- Należy upewnić się, czy gniazdko kontaktu bezpieczeństwa instalacji elektrycznej jest łatwo dostępne. Aby przerwać w pełni zasilanie prądem, wtyczka musi być wyciągnięta z gniazdka.
- Przy przyłączaniu przewodów należy przestrzegać kolejności opisanej w instrukcji obsługi. Należy używać tylko takich kabli których specyfikacje odpowiadają danym z niniejszej instrukcji obsługi lub też są dostarczone wraz z urządzeniem. W przypadku zastosowania innych przewodów firma BinTec Access Networks GmbH nie ponosi odpowiedzialności za poniesione szkody. Tym samym umowa gwarancyjna staje się nieaktualna.
- Podczas podłączania urządzenia do sieci należy przestrzegać wskazówek zawartych w instrukcji obsługi.
- Przewody należy ułożyć tak, aby nie występowało niebezpieczeństwo potykania się o nie oraz ich uszkadzania.
- Podczas burzy nie wolno podłanczać przewodów przenoszenia danych, ani też dotykać ich lub wyłanczać.

Zgodne z przeznaczeniem stosowanie, eksploatacja

- **X4100/200/300** przeznaczona jest do pracy w otoczeniu biurowym. Jako Multi-Protokoll-Router buduje **X4100/200/300** niezależnie od konfiguracji systemowej połączenia WAN. Aby zapobiec nieprzewidzianym opłatom, powinno się go strzec.

- Urządzenie **X4100/200/300** spełnia obowiązujące zasady bezpieczeństwa dla urządzeń informatycznych przeznaczonych do stosowania w otoczeniu biurowym.
- Zgodna z przeznaczeniem eksploatacja systemu zgodnie z IEC950/EN60950 jest zagwarantowana tylko w przypadku kompletnie zamontowanej obudowy blaszanej (chłodzenie, ochrona przeciwpożarowa, eliminacja zakłóceń w eterze).
- 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.
- **X4100/200/300**nie zawiera żadnych części budowy które musiałyby być wymieniane przez użytkownika, nie zawiera też żadnych przełączników czy też innych elementów które trzeba ustawiać.
- W sytuacjach awaryjnych (np. uszkodzona obudowa lub element obsługi, wniknięcie cieczy bądź ciał obcych) należy natychmiast przerwać zasilanie urządzenia prądem elektrycznym i zawiadomić serwis.

Oczyszczanie i naprawa

- Urządzenie może być otwarte tylko przez fachowca z autoryzowanego serwisu BinTec. Przed otwarciem urządzenia koniecznie wyjąć wtyczkę z gniazdka sieciowego. Otwarcie przez osoby nieupoważnione i niefachowo przeprowadzone naprawy mogą pociągnąć za sobą powstanie poważnych zagrożeń dla użytkownika (np.porażenie prądem). Naprawy mogą być wykonywane tylko przez autoryzowany serwis naprawczy BinTec. Adresy warsztatów serwisowych można uzyskać w placówkach handlowych. W pozostałych przypadkach wszelkie umowy gwarancyjne będą uznane za nieważne.
- 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.

Generelle sikkerhedsforskrifter på dansk

Nedenstående afsnit indeholder sikkerhedsforskrifter, som ubetinget skal overholdes ved brugen af apparatet.

Transport og opbevaring

- Transportér og opbevar kun **X4100/200/300** i originalemballage eller i anden egnet emballage, der beskytter mod stød og slag.

Opstilling og ibrugtagning

- Læs og overhold forskrifterne for de omgivende betingelser, før **X4100/200/300** opstilles og tages i brug (se Tekniske data). Brug et fast og jævnt underlag.
- Statisk elektricitet kan medføre apparatskader. Bær derfor en antistatisk manchet om håndleddet eller rør ved en flade med jordforbindelse, inden du rører ved stik eller udvidelseskort på **X4100/200/300**. Berør kun udvidelseskort i kanten og tag ikke fat om konstruktionsdele eller ledninger.
- Luk den ubenyttede udvidelsesmodulplads med blindafdækningen, så der ikke kan komme genstande ind i apparatets indre. Er der fremmede genstande i apparatet under driften, er der fare for elektriske stød og kortslutninger.
- Sørg for, at ingen spidse genstande beskadiger displaymodulets displayrude. Beskyt displaymodulet mod stød og fald og slut det kun til den dertil beregnede RJ11-bøsning på **X4100/200/300** for at undgå skader på **X4100/200/300** og displaymodulet.
- Ved ledningsføringen skal du sørge for, at apparatets udluftningsslidser ikke dækkes til og at der ikke skabes hindringer for ventilationen. Begrænsning af ventilationen for **X4100/200/300** kan medføre skader på apparatet. Skader, som skyldes manglende ventilation, dækkes ikke af garantien.
- Undlad at åbne basisapparatet og foretag ingen manipulationer med netdelen, da der ellers kan opstå livsfare ved elektrisk stød. Fjern ingen af basisapparatets fastgørelsesskruer.
- Hvis apparatet bringes fra kolde omgivelser ind i det rum, hvor det skal bruges, kan der opstå kondensvand både udvendigt og indvendigt på apparatet. Vent, indtil apparatet har tilpasset sig temperaturen og er absolut tørt, før du tager det i brug. Overhold omgivelsesbetingelserne i Tekniske data.

- Kontrollér, om den lokale netspænding stemmer overens med netdelens mærkespænding. Apparatet må anvendes under følgende betingelser:
  - 100 - 240 VAC
  - 50/60 Hz
- Kontrollér, at der er fri adgang til installationens jordede sikkerhedsstikkontakt. For at opnå fuld afbrydelse fra strømnettet skal netstikket trækkes ud.
- Følg den rækkefølge, der angives i denne håndbog, for tilslutningen af kablerne. Brug kun kabler som opfylder specifikationerne i denne håndbog eller de originale, medfølgede kabler. BinTec Access Networks GmbH hæfter ikke for evt. skader eller funktionsbegrænsninger ved brug af andre kabler. I sådanne tilfælde bortfalder apparatets garanti.
- Overhold henvisningerne i denne håndbog mht. apparatets tilslutning.
- Ledningerne skal trækkes på en sådan måde, at de ikke beskadiges og at de ikke er til fare for omgivelserne (fare for at snuble).
- Undlad at tilslutte eller trække datatransmissionsledninger ud af apparatet, når det er tordenvejr, og undlad at berøre dem.

Bestemmelsesmæssig anvendelse, brug

- **X4100/200/300** er beregnet til anvendelse i kontormiljø. Som multiprotokolrouter etablerer **X4100/200/300** WAN-forbindelser afhængigt af systemkonfigurationen. For at forebygge uønskede afgiftsbetalinger bør du ubetinget overvåge produktet.
- **X4100/200/300** opfylder de gældende sikkerhedsbestemmelser for informationsteknisk udstyr til kontorer.
- Bestemmelsesmæssig anvendelse af systemet iht. IEC_950/EN_60950, er kun sikret, når metalkabinettet er monteret komplet (køling, brandsikkerhed, radiostøjdæmpning).
- Omgivelsestemperaturen må ikke overstige 50 °C. Undgå direkte sollys.
- Sørg for, at genstande (f.eks. klips) eller væske ikke trænger ind i apparatet (elektrisk stød, kortslutning). Sørg for tilstrækkelig køling.
- **X4100/200/300** indeholder ingen komponenter, som må udskiftes af brugeren, eller kontakter/jumpere, som brugeren skal indstille.

- Afbryd straks strømforsyningen og kontakt serviceafdelingen i nødstilfælde (f.eks. beskadiget kabinet eller betjeningselement, indtrængning af væske eller fremmede genstande).

Rengøring og reparation

- Apparatet må kun åbnes af et BinTec-autoriseret serviceværksted. Træk altid netstikket ud, før apparatet åbnes. Uautoriseret åbning og ukorrekt udførte reparationer kan medføre betydelige farer for brugeren (f.eks. elektrisk stød). Lad kun et autoriseret BinTEC-serviceværksted udføre reparationer på apparatet. Din forhandler kan oplyse dig serviceværkstedets adresse. I alle andre tilfælde bortfalder enhver garanti.
- Apparatet må under ingen omstændigheder rengøres med væske. Indtrængende vand kan udsætte brugeren for alvorlige farer (f.eks. elektrisk stød) og forårsage alvorlige skader på apparatet.
- Benyt aldrig skuremidler, alkaliske rengøringsmidler, skrappe eller skurende hjælpemidler.

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**.

1TR6 Im deutschen ISDN verwendetes D-Kanal-Protokoll. Heute gängigeres Protokoll ist das ➤➤ **DSS1**.

Access List Eine Regel, die eine Anzahl von Datenpaketen definiert, die vom Router übertragen bzw. nicht übertragen werden sollen.

Accounting Aufzeichnen von Verbindungsdaten, wie z. B. Datum, Uhrzeit, Verbindungsdauer, Gebühreninformation und Anzahl der übertragenen Datenpakete.

Anlagenanschluß Point-to-Point (➤➤ **Punkt-zu-Punkt**)

Ein Anlagenanschluß dient zum Anschluß einer ➤➤ **TK-Anlage**. Die TK-Anlage kann Rufe an mehrere Endgeräte weiterleiten. Zu einem Anlagenanschluß gehören eine ➤➤ **Anlagenrufnummer**, über die von extern die TK-Anlage angesprochen wird und ein Bereich von Rufnummern (➤➤ **Rufnummernband**), mit denen die Endgeräte, die an der TK-Anlage angeschlossen sind, ausgewählt werden.

Anlagenrufnummer Zu einem Anlagenanschluß gehören eine Anlagenrufnummer und ein ➤➤ **Rufnummernband**. Mit Hilfe der Anlagenrufnummer erreichen Sie die TK-Anlage. Über eine Rufnummer des Rufnummernbands wird dann ein bestimmtes Endgerät der ➤➤ **TK-Anlage** ausgewählt.

ADSL Asymmetric ➤➤ **Digital Subscriber Line**

Die Datenrate beträgt ➤➤ **Upstream** bis zu 640 kBit/s und ➤➤ **Downstream** 1,5 - 9 MBit/s über Distanzen bis zu 5,5 km.

ADSL-Anwendungen sind vor allem: Internetzugang, Video-on-Demand (digital und komprimiert) und High-Speed-Datenkommunikation über ➤➤ **POTS**.

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 **X4100/200/300** die Datenübertragungsrate bei einem ISDN-Basisanschluß auf bis zu 128 kBit/s gesteigert werden.

BOD Bandwith on Demand

Bandwith on Demand ist ein erweitertes Verfahren der ➤➤ **Kanalbündelung**, bei dem es zusätzlich möglich ist, ➤➤ **Wählverbindungen** zu ➤➤ **Festverbindungen** zuzuschalten oder Wählverbindungen als Backup-Möglichkeit für Festverbindungen zu konfigurieren.

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 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-/Datennetze 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 von 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. ➤➤ **STAC**, ➤➤ **VJHC**, ➤➤ **MPPC**.

Datenpaket Ein Datenpaket dient der Übermittlung von Informationen. Jedes Datenpaket enthält eine vorgeschriebene Anzahl von Zeichen (Informationen und Steuerzeichen).

DCE Data Circuit-Terminating Equipment

Datenübertragungseinrichtung (siehe auch ➤➤ **V.24**)

DFÜ Datenfernübertragung

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 Systemadministrator festgelegt wird. Voraussetzung: ➤➤ **TCP/IP** ist bei den Clients so konfiguriert, daß die Clients ihre IP-Adresse vom Server anfordern. **X4100/200/300** 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 mitgeliefert.

D-Kanal Steuerkanal eines ➤➤ **ISDN-Basisanschlusses** bzw. ➤➤ **Primärmultiplexanschlusses**. 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 ➤➤ **Host-Namen** benutzt werden, um verschiedene Geräte anzusprechen, muß die zugehörige IP-Adresse bekanntgegeben werden. Diese Aufgabe übernimmt z. B. ein DNS Server. Er löst die Host-Namen 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).

Downstream Datenübertragungsrate vom ➤➤ **Internet Service Provider** zum Kunden.

DSL/xDSL Digital Subscriber Line

Datenübertragungstechnik, mit welcher auf gewöhnlichen Telefonleitungen hohe Übertragungsraten erreicht werden können.
Die Datenrate ist dabei von der zu überwindenden Distanz und der Leitungsqualität abhängig und variiert daher.

xDSL dient als Platzhalter für die verschiedenen DSL-Varianten, wie ➤➤ **ADSL**, ➤➤ **RADSL**, ➤➤ **VDSL**, ➤➤ **HDSL**, ➤➤ **SDSL**, ➤➤ **U-ADSL** etc., die zur Familie der DSL-Techniken gehören.

DSS1 Digital Subscriber Signalling System

Im Euro-ISDN verwendetes, gängiges D-Kanal-Protokoll.

DTE Data Terminal Equipment

Datenendeinrichtung (siehe auch ➤➤ **V.24**)

DTMF Dual Tone Multi Frequency (Tonfrequenzwahlsystem)

Methode für Wahlverfahren bei Telefonsystemen. Bei diesem Verfahren werden beim Drücken einer Taste der Telefontastatur gleichzeitig zwei Töne generiert, die von der TK-Anlage bzw. der Fernsprechstelle entsprechend ausgewertet werden.

Durchwahlbereich siehe ➤➤ **Rufnummernband**

Durchwahlnummer Eine Durchwahlnummer (Extension) ist eine interne Rufnummer für ein Endgerät oder ein Subsystem. Bei ➤➤ **Anlagenanschlüssen** ist die Durchwahlnummer in der Regel eine Rufnummer aus dem vom Telefonanbieter zugeteilten ➤➤ **Rufnummernband**. Bei Mehrgeräteanschlüssen kann es die MSN oder ein Teil der MSN sein.

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.

E1/T1 E1: Europäische Variante des ➤➤ **ISDN-**➤➤ **Primärmultiplexanschlusses** mit 2,048 MBit/s, die auch als E1-System bezeichnet wird.

T1: Amerikanische Variante des ISDN-Primärmultiplexanschlusses mit 23 Basiskanälen und einem D-Kanal (1,544 MBit/s).

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.

Extension siehe ➤➤ **Durchwahlnummer**

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 **X4100/200/300** stehen Schutzmechanismen wie ➤➤ **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**.

HDSL High Data Rate ➤➤ **DSL**

Die Datenrate beträgt ➤➤ **Upstream** und ➤➤ **Downstream** für ➤➤ **T1**: 1,554 MBit/s und für ➤➤ **E1**: 2,048 MBit/s über Distanzen bis zu 4 km.

HDSL-Anwendungen sind vor allem: High-Speed-Datenkommunikation über Festverbindungen.

HDSL2 High Data Rate ➤➤ **DSL**, Version 2

Die Datenrate beträgt ➤➤ **Upstream** und ➤➤ **Downstream** 1,554 MBit/s über Distanzen bis zu 4 km.

HDSL-Anwendungen sind vor allem: High-Speed-Datenkommunikation über Festverbindungen.

Host-Name Bezeichnet in ➤➤ **IP**-Netzen einen Namen, der als Ersatz einer zugehörigen ➤➤ **IP-Adresse** benutzt wird. Ein Host-Name besteht aus einer ASCII-Zeichenfolge, die den Host eindeutig kennzeichnet.

Hub Netzwerkkomponente, mit der mehrere Netzwerkkomponenten zu einem lokalen Netz zusammengeschlossen werden (sternförmig).

ICMP Internet Control Message Protocol

Eine Erweiterung zum Internet-Protokoll (➤➤ **IP**), die IP-bezogene Fehlermeldungen, Testpakete und Informationsmeldungen ermöglicht. Definiert in STD 5, RFC 792.

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**.

IPX/SPX Internet Packet Exchange/Sequenced Packet Exchange

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 Integrated Services Digital Network

Das ISDN ist ein digitales Netz, das die Übertragung von Sprache und Daten ermöglicht. Für ISDN gibt es zwei mögliche Teilnehmeranschlüsse, den ➤➤ **ISDN-Basisanschluß** und den ➤➤ **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 sogenannten ➤➤ **S_0-Bus** geschaffen.

ISDN-BRI ISDN Basic Rate Interface

➤➤ **ISDN-Basisanschluß**, auch ➤➤ **S_0-Anschluß**.

ISDN-Login Funktion von **X4100/200/300**. Über ISDN-Login ist **X4100/200/300** 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.

ISDN-PRI ISDN Primary Rate Interface

ISDN-➤➤ **Primärmultiplexanschluß**, auch ➤➤ **S_{2M}-Anschluß**.

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.

ITU International Telecommunication Union

Internationale Organisation, die den Aufbau und den Betrieb von Telekommunikationsnetzen/-diensten koordiniert.

Kanalbündelung Channel Bundling

Funktion von **X4100/200/300**. 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.

Mehrgeräteanschluß Point-to-Multipoint (➤➤ **Punkt-zu-Mehrpunkt**)

An einen Mehrgeräteanschluß können mehrere verschiedene Endgeräte angeschlossen werden. Die einzelnen Endgeräte werden über bestimmte Rufnummern (➤➤ **MSN**s) angesprochen.

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 herstellerspezifische Objekte. ➤➤ **SNMP** setzt auf MIB auf.

MMI Man Machine Interface

Das MMI ist eine komfortable Benutzerführung mit LCD-Display und Eingabetasten, die den Anwender durch grundlegende Funktionen von **X4100/200/300** navigiert.

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 Microsoft Point-to-Point Encryption

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. (Bei Rufnummer 49 911 7654321 entspricht z. B. die 7654321 der MSN.)

In der Regel erhält man in Deutschland mit dem ISDN-Basisanschluß (Mehrgeräteanschluß) drei solcher MSNs.

Multiprotokoll-Router ➤➤ **Router**, der mehrere Protokolle routen kann, z. B. ➤➤ **IP**, ➤➤ **IPX** etc.

NAT Network Address Translation

Sicherheitsmechanismus von **X4100/200/300**. 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**.

NT Network Termination

Ein NT-Adapter ist das Netzabschlußgerät einer ➤➤ **ISDN**-Leitung, 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. Er entspricht dem Verteilerkästchen (TAE-Dose) beim analogen Telefonanschluß.

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. Er entspricht dem Verteilerkästchen (TAE-Dose) beim analogen Telefonanschluß.

OSI-Modell OSI = Open System Interconnection (offene Kommunikationssysteme)

Referenzmodell der ➤➤ **ISO** für Netzwerke. Definiert Schnittstellenstandards zwischen Computerherstellern in den Bereichen Software- und Hardware-Anforderungen.

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**. Arbeitet 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.

POTS Plain Old Telephone System

Das traditionelle, analoge Telefonnetz.

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 Authentisierungsmechanismen über ➤➤ **PAP/CHAP**.

PPP-Authentisierung Sicherheitsmechanismus. Authentisierung durch ein Paßwort im ➤➤ **PPP**.

PPPoE Point to Point Protocol over Ethernet

Das Protokoll PPP-over-Ethernet (PPPoE) ermöglicht den Internet-Zugang via Ethernet über ein ➤➤ **xDSL**-Modem bzw. über einen xDSL-Router.

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.

RADSL Rate-adaptive ➤➤ **Digital Subscriber Line**

Die Datenrate beträgt ➤➤ **Upstream** bis zu 640 kBit/s und ➤➤ **Downstream** 1,5 - 9 MBit/s über Distanzen bis zu 18,5 km.

RADSL-Anwendungen sind vor allem: Internetzugang, Video-on-Demand (digital und komprimiert) und High-Speed Datenkommunikation über ➤➤ **POTS**.

Real Time Clock (RTC) Hardware-Uhr mit Pufferbatterie

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 **X4100/200/300**) 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 **X4100/200/300** 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.

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 Schicht 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 protokolltransparent 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 **X4100/200/300** sind ➤➤ **Multiprotokoll-Router** und dadurch in der Lage, mehrer Protokolle zu routen (z B. IP und IPX).

Rufnummernband (Durchwahlbereich)

Zu einem **Anlagenanschluß** gehören eine ➤➤ **Anlagenrufnummer** und ein Rufnummernband. Mit Hilfe der Anlagenrufnummer erreichen Sie die TK-Anlage. Beim Rufnummernband handelt es sich um einen Rufnummernbereich, mit dem Endgeräte innerhalb der ➤➤ **TK-Anlage** ausgewählt werden können.

S_0-Anschluß Siehe ➤➤ **ISDN-Basisanschluß**.

S_0-Bus Sämtliche ISDN-Anschlußdosen und der ➤➤ **NTBA** beim ISDN-Mehrgeräteanschluß. 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**.

SDSL Single Line ➤➤ **Digital Subscriber Line**

Die Datenrate beträgt ➤➤ **Upstream** und ➤➤ **Downstream** bis zu 768 kBit/s über Distanzen bis zu 3,5 km.

SDSL-Anwendungen sind vor allem: ➤➤ **E1/T1** und ➤➤ **POTS**.

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 **X4100/200/300**. Das Setup Tool kann verwendet werden, sobald ein Zugang zum Router (seriell, ➤➤ **ISDN-Login**, ➤➤ **LAN**) besteht.

Shorthold Bezeichnet die definierte Zeit, nach der 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, zu kontrollieren und zu überwachen. Mit Ihrem Router haben Sie ein solches SNMP-Werkzeug erhalten, den **Configuration Manager**. Da SNMP ein genormtes Protokoll ist, können Sie aber auch beliebige andere SNMP-Manager wie z. B. HP-Openview verwenden.

SNMP-Shell Eingabeebene für SNMP-Kommandos.

SOHO Small Offices and Home Offices

Kleine Büros und Heimarbeitsplätze.

Spoofing Technik zur Reduktion des Datenverkehrs (und damit zur Kostenersparnis) insbesondere in WANs.

Auf zyklisch ausgesendete Datenpakete mit Überwachungsfunktionen (z. B. Lebenszeichennachrichten) antwortet der Router als Proxy für ferne Rechner.

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 Ausgangs-Port. Im Gegensatz zu Bridges haben Switches allerdings mehrere Ein- und Ausgangs-Ports. 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.

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).

T-DSL Produktname der Deutschen Telekom AG für ihre ➤➤ **DSL**-Dienstleistungen und Produkte.

TE Terminal Equipment

Endgerät am Teilnehmeranschluß, z. B. Telefon, Faxgerät oder Computer.

TEI Terminal Endpoint Identifier

Der TEI im ➤➤ **ISDN** ist ein Adreßfeld der Schicht 2, um ein bestimmtes Endgerät zu identifizieren.

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.

U-ADSL Universal ➤➤ **Asymmetric Digital Subscriber Line**

Die Datenrate beträgt ➤➤ **Upstream** 128 kBit/s und ➤➤ **Downstream** 1 MBit/s über Distanzen bis zu 5,5 km.

U-ADSL-Anwendungen sind vor allem: ➤➤ **POTS** Internetzugang.

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.

Upstream Datenübertragungsrate vom Kunden zum ➤➤ **Internet Service Provider**.

URL Universal/Uniform Resource Locator

Adresse eines Files im Internet

V.11 ITU-T-Empfehlung für symmetrische Doppelstrom-Schnittstellenleitungen (bis zu 10 MBit/s)

V.24 CCITT- und ITU-T-Empfehlung, die die Schnittstelle zwischen einem Computer oder Terminal als Datenendeinrichtung (➤➤ **DTE**) und einem Modem als Datenübertragungseinrichtung (➤➤ **DCE**) definiert.

V.28 TU-T-Empfehlung für unsymmetrische Doppelstrom-Schnittstellenleitung

V.35 ITU-T-Empfehlung für Datenübertragung mit 48 kBit/s im Bereich 60-108 kHz.

V.36 Modem für ➤➤ **V.35**.

V.90 ITU-Standard für 56 kBit-Analogmodems. Im Gegensatz zu den älteren V.34-Modems werden mit dem V.90-Standard Daten digital zum Kunden weitergesendet und müssen auf einer Modemseite (Provider) nicht zuerst von digital in analog umgewandelt werden, wie es bei V.34-Modems und früheren der Fall ist. Dadurch sind höhere Übertragungsraten möglich. Eine maximale Geschwindigkeit von 56 kBit/s kann nur unter optimalen Umständen erreicht werden.

VDSL Very High Bit Rate ➤➤ **Digital Subscriber Line** (auch als VADSL oder BDSL bezeichnet)

Die Datenrate beträgt ➤➤ **Upstream** 1,5 bis 2,3 MBit/s und ➤➤ **Downstream** 13 bis 52 MBit/s über Distanzen von 300 m bis 14 km.

VDSL-Anwendungen sind vor allem: wie bei ➤➤ **ADSL**, aber mit höheren Übertragungsraten und Synchronisierung über kurze Entfernungen.

VJHC Van-Jacobsen-Header-Komprimierung

Verfahren zur ➤➤ **Datenkompression**. IP-Header-Komprimierung.

VPN Virtual Private Network

Die Nutzung bestehender Strukturen wie der des ➤➤ **Internets** zur Verbindung von privaten Netzwerken (z. B. SOHO - Zentrale). Um gesteigerten Sicherheitsanforderungen gerecht zu werden, können die Daten zwischen den beiden Endpunkten des VPN verschlüsselt werden.

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.21bis Die Empfehlungen aus X.21bis definieren die ➤➤ **DTE**/➤➤ **DCE**-Schnittstelle zu synchronen Modems der V-Serie.

X.25 Protokoll, das die Schnittstelle von Netzwerkkomponenten zu einem Paketvermittlungsnetz definiert.

X.31 zur Integration von X.25-fähigen DTEs in ISDN

FaxBack an 0911 - 6880725

Wie schätzen Sie Ihre eigenen Fähigkeiten ein?

O Netzwerkspezialist O mittlere Netzwerkkenntnisse O wenig Netzwerkkenntnisse

Wie beurteilen Sie den Umfang des Handbuchs?

O zu wenig O genau richtig O zu viel

Fehlt etwas Wichtiges im Handbuch?

O nein O ja, und zwar:.....

Gibt es Überflüssiges im Handbuch?

O nein O ja, und zwar:.....

Wie beurteilen Sie die Übersichtlichkeit des Handbuchs?

O sehr gut O gut O mittel O schlecht O sehr schlecht

Wie beurteilen Sie die Verständlichkeit des Handbuchs (Beispiele, Erklärungen, Grafiken)?

O sehr gut O gut O mittel O schlecht O sehr schlecht

Hatten Sie beim Installieren/Konfigurieren ein Problem, das Sie mit dem Handbuch nicht lösen konnten?

O nein O ja, und zwar:.....

Welche Konfigurations-Tools nutzen Sie?

O Setup Tool O Configuration Manager O SNMP-Kommandos O andere:.....

Kommentare:

.....
.....
.....
.....