



X4000

Benutzerhandbuch

Installation und Konfiguration

Copyright © 2000 BinTec Communications AG, alle Rechte vorbehalten

Version 1.3

Dokument #70000L

Juli 2000



Ziel und Zweck Dieses Handbuch beschreibt die Installation und Erstkonfiguration von **X4000** mit Software-Release 5.1.6. 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 Communications AG haftet nur im Umfang Ihrer Verkaufs- und Lieferbedingungen und übernimmt keine Gewähr für technische Ungenauigkeiten und/oder Auslassungen.

Die Informationen in diesem Handbuch können ohne Ankündigung geändert werden. Zusätzliche Informationen, sowie Änderungen und Release Notes für **X4000** finden Sie unter www.bintec.de.

Als Multiprotokollrouter baut **X4000** in Abhängigkeit von der Systemkonfiguration WAN-Verbindungen auf. Um ungewollte Gebühren zu vermeiden, sollten Sie das Produkt unbedingt überwachen. BinTec Communications AG übernimmt keine Verantwortung für Datenverlust, ungewollte Verbindungskosten und Schäden, die durch den unbeaufsichtigten Betrieb des Produkts entstanden sind.

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

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

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

Richtlinien und **X4000** entspricht folgenden Richtlinien und Normen:

Normen

- Niederspannungsrichtlinie 73/23/EWG nach EN60950, Gerätesicherheit
- Störfestigkeit nach EN50082 -1/8.97



- Störaussendung Grenzwertklasse B nach EN55022/-8.94 +A1/1995 +A2/1997, Elektromagnetische Verträglichkeit nach EU-Richtlinie 89/336/EWG

- CE-Zeichen für alle EU-Länder

Zulassungen:

- CE-Zulassungen
- TÜV/GS
- BAKOM-Zulassung (Schweiz) war zum Zeitpunkt der Drucklegung dieses Handbuchs noch nicht abgeschlossen. Beachten Sie dazu die aktuellen Release Notes unter www.bintec.de.

Zusätzlich zu den CE-Richtlinien genügt **X4000** den ISDN-Voraussetzungen in Frankreich und kann an Euro-Numeris angeschlossen werden.

Wie Sie BinTec erreichen

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





Willkommen	15
Allgemeine Sicherheitshinweise	31
Beschreibung und Installation der Hardware	35
Voraussetzungen für die Konfiguration	69
Man Machine Interface (MMI) – Display mit Benutzerführung	93
Schnelle Konfiguration mit dem Configuration Wizard (Grundgerät)	109
Grundkonfiguration des Grundgeräts mit dem Setup Tool	119
Weiterführende Konfiguration des Grundgeräts mit dem Setup Tool	193
Konfiguration der Erweiterungs- und Ressourcenkarten mit dem Setup Tool	287
Konfiguration von Sicherheitsfunktionen und Firewall	319
Konfigurationsmanagement	379
Troubleshooting	391
Technische Daten	403
Wichtige Kommandos	427
Glossar	437
Index	457



1	Willkommen	15
1.1	X4000 – Der Workgroup-Access-Router für Heute und Morgen	16
1.2	Lieferumfang	18
1.2.1	Grundgerät	18
1.2.2	Erweiterungskarten	18
1.3	BinTec Companion CD	20
1.4	Dokumentation bei BinTec	22
1.5	Systemvoraussetzungen	23
1.6	Garantiebedingungen	24
1.7	Zu diesem Handbuch	25
1.7.1	Inhalt	25
1.7.2	Verwendung	27
1.8	Feedback	29
2	Allgemeine Sicherheitshinweise	31
3	Beschreibung und Installation der Hardware	35
3.1	Grundgerät	36
3.1.1	Desktop-Gerät	37
3.1.2	19-Zoll-Einbaugerät	40
3.2	Erweiterungs- und Ressourcenkarten	53
3.2.1	Ausführung der Erweiterungskarten	53
3.2.2	Einbau und Austausch der Erweiterungskarte	55
3.3	Aufstellen und Anschließen	59
3.4	Statusmeldung über Leuchtdioden (LEDs)	63
3.4.1	Grundgerät	63
3.4.2	Erweiterungskarten	64

	3.5	Boot-Sequenz	66
4		Voraussetzungen für die Konfiguration	69
	4.1	Zugangsmöglichkeiten	70
	4.1.1	Man Machine Interface (MMI)	71
	4.1.2	Zugang über die serielle Schnittstelle	71
	4.1.3	Zugang über LAN	73
	4.1.4	Zugang über ISDN	74
	4.2	Anmelden	76
	4.3	Konfigurationsmöglichkeiten	78
	4.3.1	Übersicht	78
	4.3.2	Bedienung des Setup Tools	80
	4.4	Vorgehensweise für Initialkonfiguration	91
5		Man Machine Interface (MMI) – Display mit Benutzerführung	93
	5.1	Überblick	94
	5.2	Display und Eingabetasten	96
	5.2.1	Eingabetasten verwenden	96
	5.2.2	Bedeutung der LEDs	97
	5.2.3	Navigationsleisten	98
	5.3	Menüstruktur	99
	5.3.1	Display-Einstellungen	100
	5.3.2	IP-Adresse und Netzmaske	102
	5.3.3	Datum und Systemzeit	103
	5.3.4	Angaben zum Grundgerät	104
	5.3.5	Angaben zur Erweiterungskarte	105
	5.3.6	Monitoring	106
	5.4	Nützliche Short-Cuts	107
	5.4.1	Default-Screen festlegen	107
	5.4.2	Konfiguration sichern	107

5.4.3	X4000 neustarten	108
6	Schnelle Konfiguration mit dem Configuration Wizard (Grundgerät)	109
6.1	Konfiguration vorbereiten	111
6.2	BRICKware installieren	113
6.3	Grundlegende X4000 -Konfiguration mit dem Configuration Wizard	114
6.4	PC einrichten	116
6.5	Konfiguration testen	118
7	Grundkonfiguration des Grundgeräts mit dem Setup Tool	119
7.1	Grundlegende Routereinstellungen	120
7.1.1	Lizenz(en) eintragen	121
7.1.2	Systemdaten eintragen	123
7.1.3	LAN-Schnittstelle konfigurieren	126
7.1.4	X4000 als DHCP-Server einrichten	129
7.1.5	Filter setzen	132
7.1.6	Wie geht's jetzt weiter?	136
7.2	WAN-Schnittstellen konfigurieren	138
7.2.1	ISDN-BRI-Schnittstelle konfigurieren	138
7.2.2	Serielle Schnittstellen konfigurieren	151
7.2.3	LAN-Schnittstelle zur Nutzung von ADSL konfigurieren (PPP-over-Ethernet)	157
7.3	WAN-Partner einrichten	162
7.3.1	Prinzipielle Vorgehensweise	162
7.3.2	Beispiele	187
7.4	Konfigurationsdatei sichern	191

8	Weiterführende Konfiguration des Grundgeräts mit dem Setup Tool	193
8.1	Allgemeine WAN-Einstellungen	194
8.1.1	Dynamic IP Address Server	194
8.1.2	CAPI User Concept	196
8.1.3	Allgemeine PPP-Einstellungen	200
8.1.4	X.31 TEI	203
8.2	WAN-Partner-spezifische Einstellungen	204
8.2.1	Delay after Connection Failure	204
8.2.2	Channel Bundling	205
8.2.3	Bandwidth on Demand (BOD)	207
8.2.4	Always On/Dynamic ISDN (AO/DI)	213
8.2.5	Layer 1 Protocol (ISDN-B-Kanal)	226
8.2.6	IP Transit Network	229
8.2.7	Übermittlung von DNS- und WINS-Server-IP-Adressen an WAN-Partner	232
8.2.8	Routing Information Protocol (RIP)	236
8.2.9	Komprimierung	239
8.2.10	Proxy ARP (Address Resolution Protocol)	241
8.2.11	Keepalive Monitoring	243
8.3	Grundlegende IP-Einstellungen	249
8.3.1	Systemzeit	249
8.3.2	Namensauflösung - X4000 mit DNS-Proxy	254
8.3.3	Portnummern	274
8.3.4	BOOTP Relay Agent	275
8.4	IPX-Einstellungen	278
8.4.1	Allgemeine Einstellungen	278
8.4.2	LAN-Schnittstelle konfigurieren	280
8.4.3	WAN-Partner einrichten	281
8.5	Bridging	285
8.6	Features mit Zusatzlizenz	286

9	Konfiguration der Erweiterungs- und Ressourcenkarten mit dem Setup Tool	287
9.1	WAN-Schnittstellenkarte für ISDN-BRI	288
9.1.1	Konfiguration mit dem Setup Tool	288
9.2	WAN-Schnittstellenkarte für ISDN-PRI und/oder G.703	292
9.2.1	Konfiguration mit dem Setup Tool	293
9.3	LAN-Schnittstellenkarte für 10/100 MBit/s	298
9.3.1	Konfiguration mit dem Setup Tool	298
9.3.2	Breitband-Internetzugang (ADSL) mit X4000 und LAN-Erweiterungskarte	299
9.4	Ressourcenkarte mit Digitalmodems	306
9.4.1	X4000 mit Digitalmodems als Remote-Access-Server	306
9.5	Ressourcenkarte zur Verschlüsselung und Kompression	317
9.5.1	Konfiguration mit dem Setup Tool	317
10	Konfiguration von Sicherheitsfunktionen und Firewall	319
10.1	Überwachen von Aktivitäten	320
10.1.1	Syslog-Messages	320
10.1.2	Monitorfunktionen im Setup Tool	325
10.1.3	Credits Based Accounting System (Taschengeldkonto)	328
10.1.4	HTTP-Statusseite	332
10.1.5	Java-Statusmonitor	334
10.1.6	Activity Monitor	334
10.2	Zugangssicherung	338
10.2.1	Anmelden	338
10.2.2	Überprüfen der eingehenden Rufnummer	339
10.2.3	Authentisierung von PPP-Verbindungen mit PAP, CHAP oder MS-CHAP	340
10.2.4	Callback	341
10.2.5	Closed User Group	343
10.2.6	Zugriff auf Remote-CAPI	343
10.2.7	NAT (Network Address Translation)	344

10.2.8	Filter (Access Lists)	349
10.2.9	Lokale Filter	363
10.2.10	Backroute Verification	367
10.2.11	TAF-Client	368
10.2.12	Extended IP-Routing (XIPR)	368
10.3	Abhörsicherung	370
10.3.1	Verschlüsselung	370
10.3.2	VPN (mit Zusatzlizenz)	373
10.4	Besonderheiten	374
10.4.1	Startup-Verhalten	374
10.4.2	Auto-Logout	374
10.4.3	Vorbeugung gegen Denial-of-Service-Attacken	374
10.5	Checkliste	376
11	Konfigurationsmanagement	379
11.1	Konfigurationsdateien verwalten	380
11.2	Software-Update durchführen	388
12	Troubleshooting	391
12.1	Hilfsmittel zum Troubleshooting	392
12.1.1	Man Machine Interface (MMI)	392
12.1.2	Lokale SNMP-Shell-Kommandos	392
12.1.3	Externe Hilfsmittel	393
12.2	Typische Fehlersituationen und Vorgehensweise	395
12.2.1	System-Fehler	395
12.2.2	ISDN-Verbindungen	396
12.2.3	IPX-Routing	399

13	Technische Daten	403
13.1	Netzteil	404
13.2	Leistungsmerkmale des Grundgeräts	405
13.2.1	Serielle Konsolenschnittstelle	406
13.2.2	Ethernet/LAN-Schnittstelle	407
13.2.3	ISDN-BRI-Schnittstelle	408
13.2.4	Serielle WAN-Schnittstellen	409
13.2.5	Display-Schnittstelle	421
13.3	Leistungsmerkmale der Erweiterungs- und Ressourcenkarten	422
13.3.1	X4E-2/3BRI – WAN-Schnittstellenkarte für ISDN-BRI (Basic Rate Interface)	422
13.3.2	X4E-1/2PRI – WAN-Schnittstellenkarte für ISDN-PRI (Primary Rate Interface) und/oder G.703	423
13.3.3	X4E-2FE – LAN-Schnittstellenkarte für 10/100 MBit/s	424
13.3.4	XTR-S/M/L – Ressourcenkarten mit Digitalmodems	425
13.3.5	XTR-ENC – Ressourcenkarte zur Verschlüsselung und Kompression	425
14	Wichtige Kommandos	427
14.1	SNMP-Shell-Kommandos	428
14.2	BRICKtools for Unix-Kommandos	435

1 Willkommen

Mit **X4000** haben Sie sich zum Kauf eines erweiterbaren Multiprotokoll-Routers aus der Workgroup-Access-Reihe von BinTec Communications AG entschieden – eine leistungsfähige und zukunftssichere Router-Lösung für den Einsatz in kleinen und mittleren Betrieben.



Bild 1-1: **X4000** - Der Workgroup-Access-Router für heute und morgen

X4000 kann mit nur einem Grundgerät vielfältige Applikationen realisieren:

- Router für Festverbindungen mit ISDN-Backup
- Zentrales Fax-Gateway für bis zu 30 Verbindungen
- Router für analoge und digitale Verbindungen
- VPN-Lösung mit Datenverschlüsselung und ISDN-Backup
- Remote-Access-Server für bis zu 62 Verbindungen

1.1 X4000 – Der Workgroup-Access-Router für Heute und Morgen

Die Erweiterbarkeit von **X4000** macht den Multiprotokollrouter zu einer zukunftssicheren und flexibel einsetzbaren Investition. Ausgestattet mit einer RISC-CPU ist **X4000** extrem leistungsfähig und auch zukünftigen Anforderungen gewachsen.

- Grundgerät** Das Grundgerät ist wahlweise als Desktop-Gerät und als 19-Zoll-Einbaugerät erhältlich. In beiden Varianten ist schon im Grundgerät eine 10/100 BT-Ethernet-Schnittstelle, eine ISDN-BRI-Schnittstelle, eine serielle X.21/V.35/V.36-Schnittstelle für Festverbindungen, eine serielle X.21bis-Schnittstelle und eine serielle Konsolenschnittstelle integriert.
- Erweiterungskarten** Ein Steckplatz für eine von außen steckbare Erweiterungskarte ermöglicht **X4000**, mit Ihren Anforderungen zu wachsen und mit dem gleichen Grundgerät verschiedene Applikationen einzusetzen. Hohe Flexibilität ist gewährleistet und es gilt: "Wechseln Sie die Karte, nicht das Gerät!"
- Ressourcenkarten** Erweiterungskarten mit ISDN-BRI- bzw. ISDN-PRI-Schnittstellen können zusätzlich mit leistungsfähigen Ressourcenkarten mit Digitalmodems ausgestattet werden. So kann eine außerordentlich hohe Leistungsfähigkeit und Port- bzw. Modemdichte erreicht werden.
- Ergonomisches Design** Ein ergonomisches und anwenderfreundliches Design ist gegeben durch die erprobte BinTec-Router-Konfigurationsoberfläche "Setup Tool" und dem "Configuration Wizard" für eine schnelle Grundkonfiguration. Das von BinTec Communications AG neu entwickelte Man Machine Interface (MMI) mit einem LCD-Display, Eingabetasten und einer intuitiven Benutzerführung – in mehreren Sprachen – erleichtert zusätzlich den "ersten Kontakt" zu Ihrem Router und das schnelle Zugreifen bzw. Anzeigen der wichtigsten Einstellungen. Darüberhinaus ermöglicht ein lüfterloses Wide-Range-Netzteil einen geräuschlosen Betrieb von **X4000** in Bürourgebungen.
- Multiprotokollrouter** Der flexible Multiprotokollrouter kann für den WAN-Access, aber auch als Remote-Access-Server, Fax-Gateway, Remote-CAPI-Server oder LAN-Router eingesetzt werden. **X4000** unterstützt die Protokolle TCP/IP, IPX und X.25 (op-

tional) und beherrscht das Bridging von weiteren Protokollen nach dem Spanning-Tree-Verfahren.

Remote-CAPI Mit Hilfe von BinTec's 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 Zugangspañwörter. Die Sicherheitsfunktionen schützen **X4000** und das daran angeschlossene Netzwerk vor unerlaubtem Zugriff.

Zukunft Neue Technologien und Entwicklungen sind der BinTec Communications AG ein Anliegen. Die flexible Plattform von **X4000** mit einem Erweiterungssteckplatz und der leistungsfähige Prozessor ermöglichen den kurzfristigen Einsatz von neuen WAN-/LAN-Technologien und Features. Somit ist **X4000** ein zukunftsicheres und migrationsfähiges Gerät. Wir bleiben dran!

Aktuelle Software wird von BinTec 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

1.2.1 Grundgerät

Das **X4000**-Grundgerät ist in der Variante Desktop-Gerät und 19-Zoll-Einbaugerät erhältlich.

Zusammen mit dem **X4000**-Grundgerät werden folgende Teile ausgeliefert:

- Kabelsätze
 - Serielles Anschlußkabel für den Konsolenport
 - Kaltgeräte-Netzkabel
 - ISDN-Kabel
- BinTec Companion CD
- Dokumentation
 - Benutzerhandbuch
 - Release Notes, falls erforderlich
- Zusätzliches Material
 - Satz 19-Zoll-Befestigungsmaterial (nur bei 19-Zoll-Einbaugerät)
 - Lizenzkarte mit Lizenzinformation
 - Einzelplatzlizenz für RVS-COM Lite
 - Beiblatt mit **X4000**-Garantieinformationen

1.2.2 Erweiterungskarten

Folgende Erweiterungskarten für **X4000** können erworben werden:

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

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

1.3 BinTec Companion CD

Auf Ihrer BinTec Companion CD finden Sie alle Programme, die Sie zur Installation, Konfiguration und Wartung von **X4000** brauchen.

BRICKware BRICKware for Windows enthält die Windows-Hilfsprogramme:

- Die DIME Tools dienen der Überwachung und Administration von **X4000**.
- Der Configuration Wizard führt Sie Schritt für Schritt durch die Grundkonfiguration von **X4000**.
- Über das Terminal-Programm BRICK at COM1 bzw. BRICK at COM2 erhalten Sie Zugang zu **X4000** 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 alle SNMP-Tabellen und -Variablen einsehen und bearbeiten.
- Mit dem Java-Statusmonitor können Sie über einen Internet Browser Systeminformationen abfragen.
- Remote-CAPI-Client:
Mit dem Remote-CAPI-Client können Sie Kommunikationsanwendungen nutzen, die auf die genormte CAPI-Schnittstelle aufsetzen (z. B. RVS-COM Lite).
- Token Authentication Firewall (TAF) Programm (optional):
Dieses Softwarepaket benötigen Sie, wenn Sie das Sicherheitssystem von Security Dynamics verwenden.
- Mit dem Activity Monitor können Sie die Auslastung von **X4000** mit einem Blick überwachen.

Genauere Beschreibungen aller Softwareprogramme finden Sie in unserem Online-Handbuch [BRICKware for Windows](#).

RVS-COM Lite Zusätzlich zur BRICKware ist auf Ihrer BinTec Companion CD das Kommunikationsprogramm RVS-COM Lite enthalten, das Ihnen typische Kommunikationsanwendungen wie z. B. Anrufbeantworter, Fax oder Dateitransfer auf Ihrem Rechner ermöglicht.



Bitte beachten Sie: Es handelt sich dabei um eine Einzelplatzlizenz für RVS-COM Lite. Weitere Lizenzen können Sie über Ihren Händler beziehen.

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 22](#))
- Eine Kopie der Router-Software
- UNIX-Tools (Administration)
- Adobe's Acrobat Reader
- Konfigurationsbeispiele

1.4 Dokumentation bei BinTec

Die Dokumentation haben Sie zusammen mit **X4000** teilweise in gedruckter und komplett in elektronischer Form (PDF, HTML) erhalten. Die elektronischen Fassungen der verschiedenen Dokumente finden Sie auf Ihrer BinTec Companion CD. Zusätzlich zur Companion CD stehen alle Dokumente jeweils in der aktuellsten Version auf unserem WWW-Server unter www.bintec.de zum Download bereit. Derzeit ist folgende Dokumentation verfügbar:

- Benutzerhandbuch (deutsch)
Dieses Handbuch.
- User's Guide (englisch)
Dieses Handbuch in englischer Sprache.
- Referenzhandbücher (englisch, PDF/HTML)
 - Software Reference (PDF)
Online-Nachschlagewerk mit tiefergehenden Informationen zu hier beschriebenen Funktionen, Nachschlagewerk für die internen SNMP-Tabellenstrukturen und die Bedienung der SNMP-Shell.
 - Extended Features Reference (PDF)
Online-Nachschlagewerk für zusätzliche, z. T. nur mit separater Lizenz verfügbare Funktionen (z. B. VPN).
 - MIB Reference
HTML-Dokument mit Kurzbeschreibungen zu allen SNMP-Tabellen und Variablen von **X4000**.
- BRICKware for Windows (englisch, PDF)
Bedienungsanleitung für die Windows-Hilfsprogramme (BRICKware)
- Release Notes (englisch, PDF und/oder gedruckt)
Aktuelle Informationen und Hinweise zum aktuellen Software-Release, Beschreibung aller Änderungen gegenüber dem vorherigen Release. Im Dokument Release Note Logic finden Sie eine Anleitung zum Upgrade von Bootmonitor und/oder Firmware-Logic.
- Release Notes für den Routerbetrieb in UK (englisch, PDF)
Hinweise zum Betrieb von BinTec-Routern in Großbritannien.

1.5 Systemvoraussetzungen

X4000 können Sie von allen herkömmlichen Plattformen aus konfigurieren. Als Standalone-Gerät ist **X4000** nicht vom angeschlossenen Rechner oder dessen Betriebssystem abhängig. Die Kommunikation zum Rechner erfolgt über 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.

Speziell für die Verwendung des Configuration Wizard benötigen Sie:

- Rechner mit serieller Schnittstelle (V.24)
- Windows 95 bzw. 98 oder Windows NT 4.0
- Installierte Netzwerkkarte (10 Mbps Ethernet oder 10/100 Mbps Fast Ethernet)
- Installiertes Microsoft TCP/IP-Protokoll
- Für die korrekte Darstellung der Grafiken benötigen Sie mehr als 256 Farben.

1.6 Garantiebedingungen

2 Jahre **X4000** hat 2 Jahre Garantie ab Kaufdatum. Zur Garantieabwicklung wenden Sie sich bitte an Ihren Händler.

6 Jahre Sie können die Garantie für **X4000** auf 6 Jahre verlängern, indem Sie sich bei BinTec Communications AG registrieren lassen. Dazu füllen Sie das dafür vorgesehene Online-Formular auf www.bintec.de aus und erhalten daraufhin umgehend eine schriftliche Bestätigung zugeschickt. Als registrierter User haben Sie nicht nur den Vorteil einer verlängerten Garantie, Sie können sich auch regelmäßig über Produkt-Neuheiten informieren lassen, wenn Sie dies wünschen.

Beachten Sie bitte das mitgelieferte Beiblatt mit detaillierten **X4000**-Garantieinformationen.



Gefahr!

Beim geöffnetem Gerät sind netzspannungsführende Bauteile zugänglich. Es besteht Lebensgefahr!

Zum Anschließen, Betreiben und auch zum Ein- bzw. Ausbau der Erweiterungskarten ist das Öffnen des Gehäuses nicht erforderlich. Falls das Gehäuse dennoch geöffnet wird, reißt das Garantielabel an **X4000** und damit erlischt die Garantie.

➤ Öffnen Sie keinesfalls das Gehäuse!

1.7 Zu diesem Handbuch

1.7.1 Inhalt

Das Handbuch ist folgendermaßen aufgebaut:

Kapitel	Inhalt
1: "Willkommen"	Allgemeine Einführung, Lieferumfang, Garantiebedingungen, Informationen zu diesem Handbuch.
2: "Allgemeine Sicherheitshinweise"	Allgemeine Sicherheitshinweise in deutsch.
3: "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 umstücken 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: "Schnelle Konfiguration mit dem Configuration Wizard (Grundgerät)"	Wie Sie X4000 mit dem Windows-Tool Configuration Wizard in wenigen Minuten in Betrieb nehmen und wie Sie weitere nützliche Software installieren und einrichten.
7: "Grundkonfiguration des Grundgeräts mit dem Setup Tool"	Wie Sie X4000 mit dem Setup Tool in Betrieb nehmen und eine Grundkonfiguration einrichten (einschließlich der Konfiguration der WAN-Schnittstellen).

Kapitel	Inhalt
8: "Weiterführende Konfiguration des Grundgeräts mit dem Setup Tool"	Wie Sie weitere Konfigurationseinstellungen mit dem Setup Tool vornehmen.
9: "Konfiguration der Erweiterungs- und Ressourcenkarten mit dem Setup Tool"	Wie Sie eine Erweiterungskarte und gegebenenfalls Ressourcenkarte(n) konfigurieren.
10: "Konfiguration von Sicherheitsfunktionen und Firewall"	Wie Sie Sicherheitsmechanismen von SAFER-NET einrichten, z. B. NAT (Network Address Translation) oder Filter.
11: "Konfigurationsmanagement"	Wie Sie Konfigurationsdateien verwalten und Software-Updates durchführen.
12: "Troubleshooting"	Wichtige Hinweise zur Fehlerbehebung.
13: "Technische Daten"	Die Technischen Daten von X4000 .
14: "Wichtige Kommandos"	Eine Kurzübersicht zu den wichtigsten Befehlen und Kommandos der SNMP-Shell und der BRICKtools für Unix.

Tabelle 1-1: Kapitelübersicht

1.7.2 Verwendung

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

Symbol	Verwendung
	Kennzeichnet Stellen, an denen Tips und Tricks verraten werden.
	Kennzeichnet Stellen, an denen Hinweise zur Fehlerbehebung gegeben werden.
	Kennzeichnet allgemeine wichtige Hinweise.
	Kennzeichnet Stellen, an denen wichtige Grundlagen erläutert werden.
	<p>Kennzeichnet Warnhinweise. Einteilung der Gefahrenstufen gemäß ANSI:</p> <ul style="list-style-type: none"> ■ Achtung (weist auf mögliche Gefahr hin, die bei Nichtbeachten Sachschäden zur Folge haben kann) ■ Warnung (weist auf mögliche Gefahr hin, die bei Nichtbeachten Körperverletzung zur Folge haben kann) ■ Gefahr (weist auf Gefahr hin, die bei Nichtbeachten Tod oder schwere Körperverletzung zur Folge haben wird)

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	Kennzeichnung von Menüs und Untermenüs im Setup Tool.
nicht-proportional (Courier), z. B. ping 192.168.1.254	■ Kennzeichnung von Kommandos (z. B. in der SNMP-Shell), die Sie wie dargestellt eingeben müssen. ■ Darstellung des Setup Tool.
<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.
<i>kursiv, z. B.</i> none	Kennzeichnung von Werten, die Sie im Setup Tool oder bei MIB-Variablen eintragen bzw. eingestellt werden können.

Tabelle 1-3: Auszeichnungselemente

1.8 Feedback

Als Dokumentationsteam bei BinTec Communications AG schreiben wir Handbücher und andere Dokumentationen für Sie. Wir wollen zu einem hochwertigen Produkt wie **X4000** 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 - 9673 1498

■ per Post an:
BinTec Communications AG
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

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

- Transport und Lagerung**
- Transportieren und lagern Sie **X4000** nur in der Originalverpackung oder in einer anderen geeigneten Verpackung, die Schutz gegen Stoß und Schlag gewährt.
- Aufstellen und in Betrieb nehmen**
- Beachten Sie vor dem Aufstellen und Betrieb von **X4000** 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 **X4000** 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 Blindabdeckung 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 **X4000** an, um Schäden an **X4000** 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 **X4000** 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 temperatur angeglichen und absolut trocken 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 Communications AG 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.
- **X4000** ist für den Einsatz in einer Büroumgebung bestimmt. Als Multiprotokoll-Router baut **X4000** in Abhängigkeit von der Systemkonfiguration WAN-Verbindungen auf. Um ungewollte Gebühren zu vermeiden, sollten Sie das Produkt unbedingt überwachen.
- **X4000** entspricht den einschlägigen Sicherheitsbestimmungen für Einrichtungen der Informationstechnik für den Einsatz in einer Büroumgebung.

Bestimmungsgemäße Verwendung, Betrieb

- 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.
- **X4000** 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.

3 Beschreibung und Installation der Hardware

Dieses Kapitel enthält folgende Informationen, die Sie zur Installation von **X4000** benötigen:

- Grundgerät, [Kapitel 3.1, Seite 36](#)
 - **X4000** als Desktop-Gerät, [Kapitel 3.1.1, Seite 37](#) oder 19-Zoll-Einbaugerät, [Kapitel 3.1.2, Seite 40](#)
 - "Display und Eingabetasten", [Seite 37](#)
 - "Einbau in einen 19-Zoll-Schrank", [Seite 40](#)
 - "Ausbau aus einem 19-Zoll-Schrank", [Seite 44](#)
- Erweiterungs- und Ressourcenkarten, [Kapitel 3.2, Seite 53](#)
 - Ausführung der Erweiterungskarten, [Kapitel 3.2.1, Seite 53](#)
 - Einbau und Austausch der Erweiterungskarte, [Kapitel 3.2.2, Seite 55](#)
- Aufstellen und Anschließen von **X4000**, [Kapitel 3.3, Seite 59](#)
 - "X4000 an PC oder Terminal anschließen", [Seite 60](#)
 - "X4000 an LAN anschließen", [Seite 60](#)
 - "X4000 an WAN anschließen", [Seite 60](#)
 - "X4000 an die Stromversorgung anschließen", [Seite 61](#)
 - Anschließen der "Erweiterungskarte", [Seite 61](#)
 - Aktivieren der "Real-Time-Clock", [Seite 61](#)
- Statusmeldungen über Leuchtdioden (LEDs), [Kapitel 3.4, Seite 63](#)
 - Grundgerät, [Kapitel 3.4.1, Seite 63](#)
 - Erweiterungskarten, [Kapitel 3.4.2, Seite 64](#)
- Boot-Sequenz, [Kapitel 3.5, Seite 66](#)

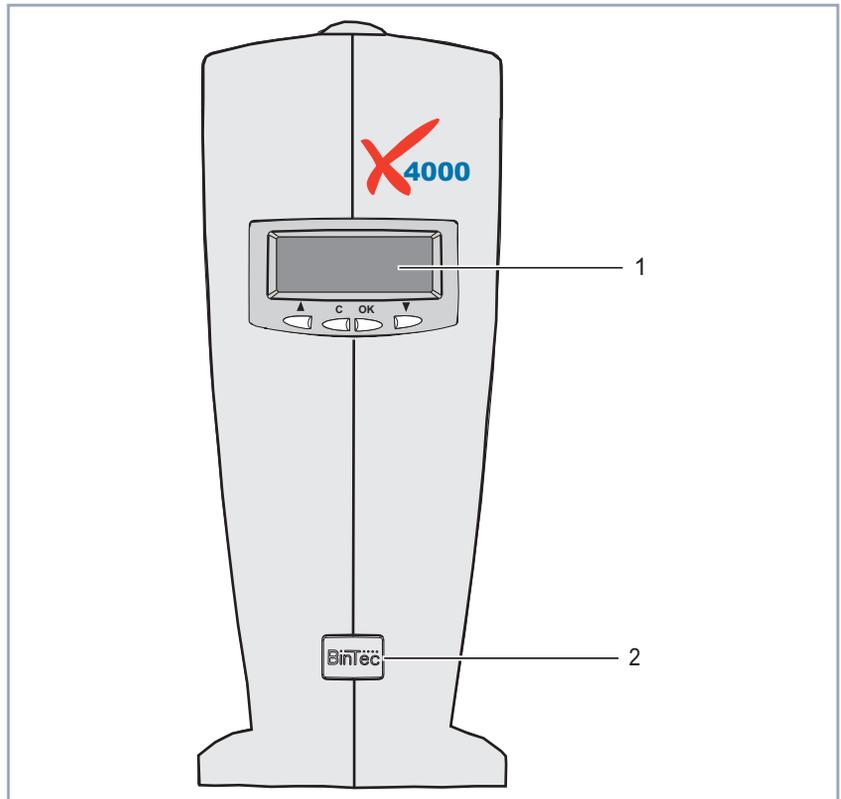
3.1 Grundgerät

BinTec Communications AG bietet Ihnen **X4000** in zwei Gerätevarianten an:

- Desktop-Gerät zum Aufstellen im Office
- Einbaugerät für den 19-Zoll-Schrank

Das **X4000**-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 Desktop-Gerät



1	Display mit Eingabetasten	2	Power-LED (blau)
---	---------------------------	---	------------------

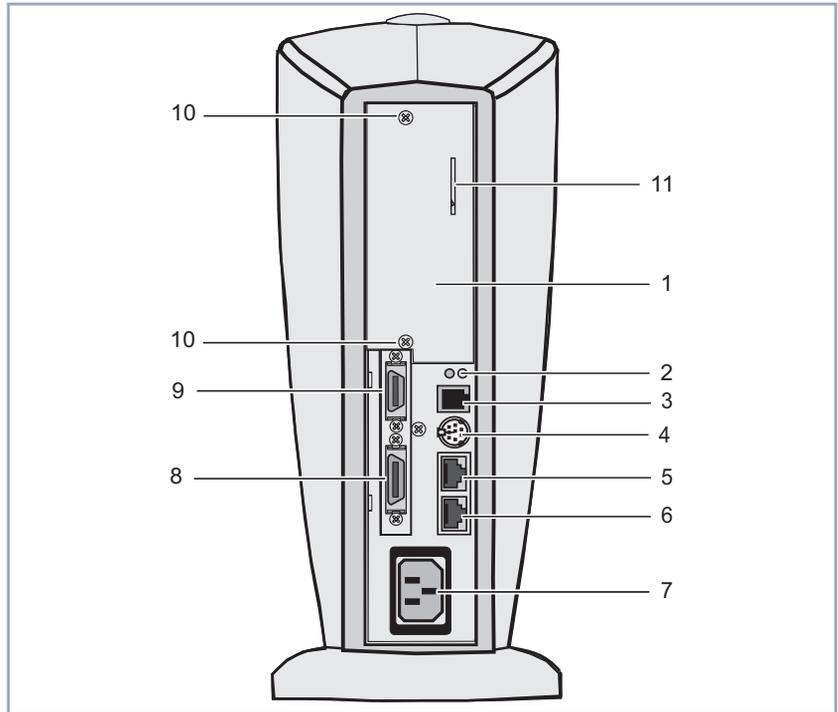
Bild 3-1: Vorderansicht Desktop-Gerät

Display und Eingabetasten

BinTecs Man Machine Interface (MMI), eine komfortable Benutzerführung mit Display und Eingabetasten, führt den Anwender durch einige grundlegende Funktionen von **X4000**. Die genaue Funktionsbeschreibung des MMI finden Sie in [Kapitel 5, Seite 93](#).

Display-Baugruppe am 19-Zoll-Einbaugerät Die Display-Baugruppe kann am 19-Zoll-Einbaugerät an der Vorderseite sowie an der Rückseite von **X4000** montiert werden. Die Umbauanleitung finden Sie in ["Schritt 2: Umstecken des Displays", Seite 47](#).

Rückansicht des Desktop-Geräts:



1	Erweiterungskartensteckplatz (mit Blindabdeckung)	7	Kaltgerätebuchse des Netzteils
2	Status-LEDs (rot und grün)	8	X.21/V.35/V.36-Schnittstelle
3	RJ11-Buchse für Display	9	X.21bis-Schnittstelle
4	Mini-DIN-Buchse (Konsole)	10	Befestigungsschrauben der Erweiterungskarte bzw. der Blindabdeckung
5	Ethernet/LAN-Schnittstelle 10/100 Base-T-Fast Ethernet	11	Kunststoffstreifen zum Aktivieren der Pufferbatterie für die Real-Time-Clock (RTC)
6	ISDN-BRI-Schnittstelle		

Bild 3-2: Rückansicht Desktop-Gerät

Zum Anschließen Ihres Desktop-Geräts gehen Sie zu [Kapitel 3.3, Seite 59](#).

3.1.2 19-Zoll-Einbaugerät

Einbau in einen 19-Zoll-Schrank Für den Einbau in einen 19-Zoll-Schrank bietet BinTec Ihnen **X4000** als 19-Zoll-Einbaugerät an.

Im folgenden wird beschrieben, wie Sie Ihr 19-Zoll-Einbaugerät in den 19-Zoll-Schrank einbauen können. **X4000** ist flexibel und kann

- mit der Frontblende nach vorne und den Anschlüssen nach hinten in Ihren 19-Zoll-Schrank eingebaut werden (vgl. "[Einbau mit Frontblende nach vorne](#)", [Seite 41](#) und [Bild 3-6, Seite 44](#)).
- mit den Anschlüssen nach vorne in Ihren 19-Zoll-Schrank eingebaut werden. Das Display kann hierbei umgesteckt werden und ist somit frontal sichtbar (vgl. "[Einbau mit Anschlüssen nach vorne und Umstecken des Displays](#)", [Seite 45](#)).

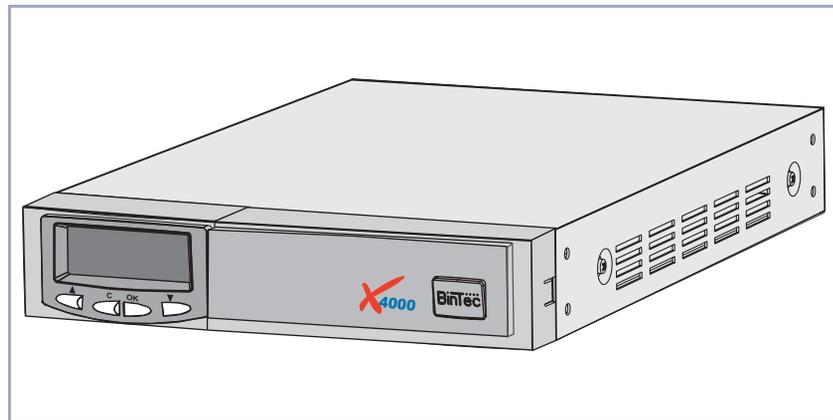


Bild 3-3: 19-Zoll-Einbaugerät

Einbau mit Frontblende nach vorne



Achtung!

Zum Anschließen, Betreiben und auch zum Ein- bzw. Ausbau der Erweiterungskarte ist das Öffnen des Gehäuses nicht erforderlich.

Falls das Gehäuse dennoch geöffnet wird, reißt das Garantielabel an **X4000** und damit erlischt die Garantie.

➤ Öffnen Sie keinesfalls das Gehäuse!

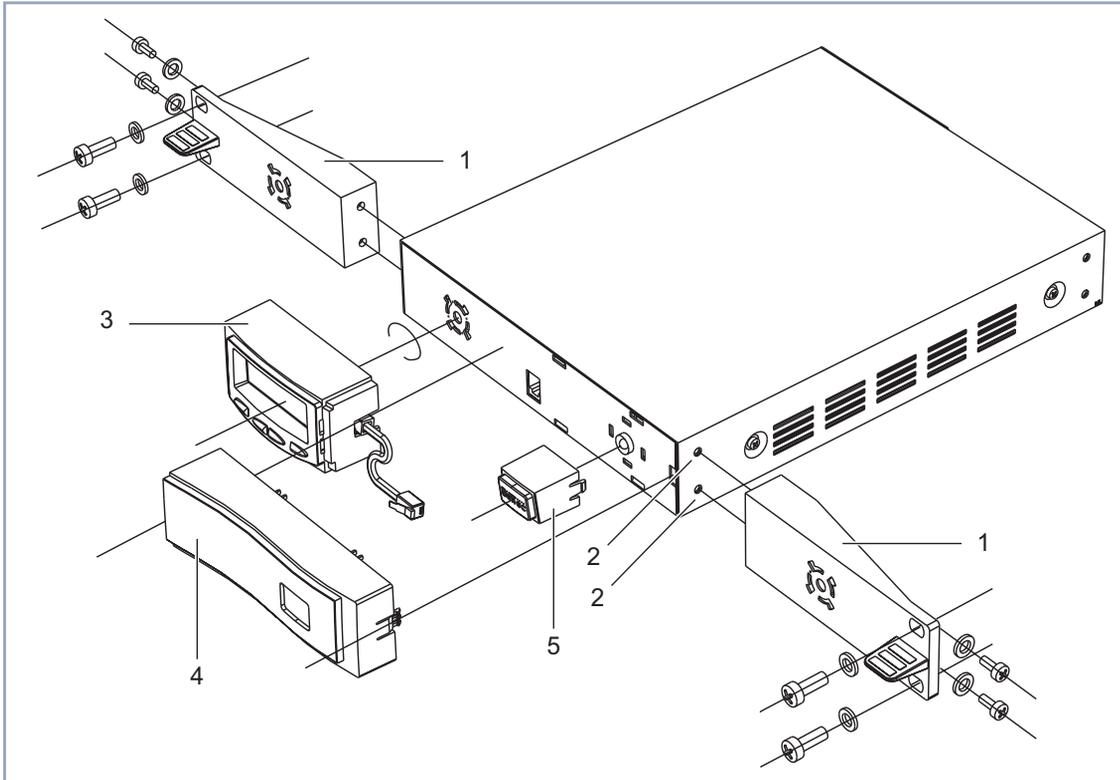


Gefahr!

Beim geöffnetem Gerät sind netzspannungsführende Bauteile zugänglich. Es besteht Lebensgefahr!

➤ Öffnen Sie keinesfalls das Gehäuse!

Folgende Bau- und Befestigungsteile benötigen Sie für den Einbau in einen 19-Zoll-Schrank:



1	Befestigungswinkel	4	Blende
2	Befestigungslöcher	5	Power-LED-Gehäuse
3	Display-Baugruppe		

Bild 3-4: Explosionszeichnung mit den wichtigsten Bau- und Befestigungsteilen für den Einbau von **X4000** in einen 19-Zoll-Schrank

Gehen Sie folgendermaßen vor:

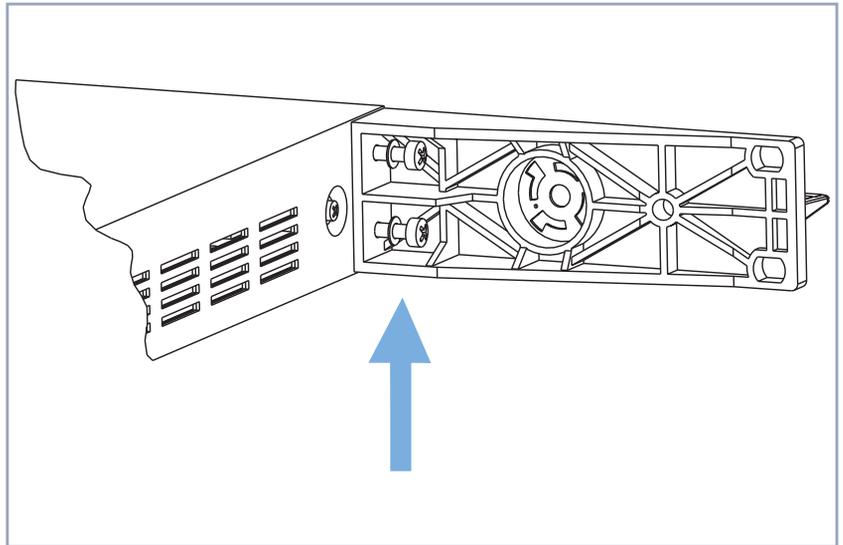


Bild 3-5: Winkel an Befestigungslöcher festschrauben

- Schritt 1** ➤ Schrauben Sie die beiden mitgelieferten Befestigungswinkel mit den mitgelieferten Schrauben an die vorderen, seitlich von **X4000** dafür vorgesehenen Befestigungslöcher von **X4000** fest, siehe [Bild 3-5, Seite 43](#). Verwenden Sie unbedingt die mitgelieferten Schrauben. Andere Schrauben halten eventuell den mechanischen Belastungen nicht stand oder können das Gerät zerstören.
- Schritt 2** ➤ Stecken Sie die benötigten Schnittstellenkabel in die dafür vorgesehenen Buchsen (Kabel müssen bereits verlegt sein, wenn Ihr Schrank von hinten nicht zugänglich ist!).
- Schritt 3** ➤ Schieben Sie diese vormontierte Einheit mit den beiden angeschraubten Winkeln in Ihren Schrank und verschrauben Sie die vormontierte Einheit mit den Längsprofilen des Schrankes (diese Schrauben sind nicht im Lieferumfang von **X4000** enthalten, sondern sind Bestandteil des Schranklieferumfangs).

So sollte **X4000** fertig montiert aussehen:

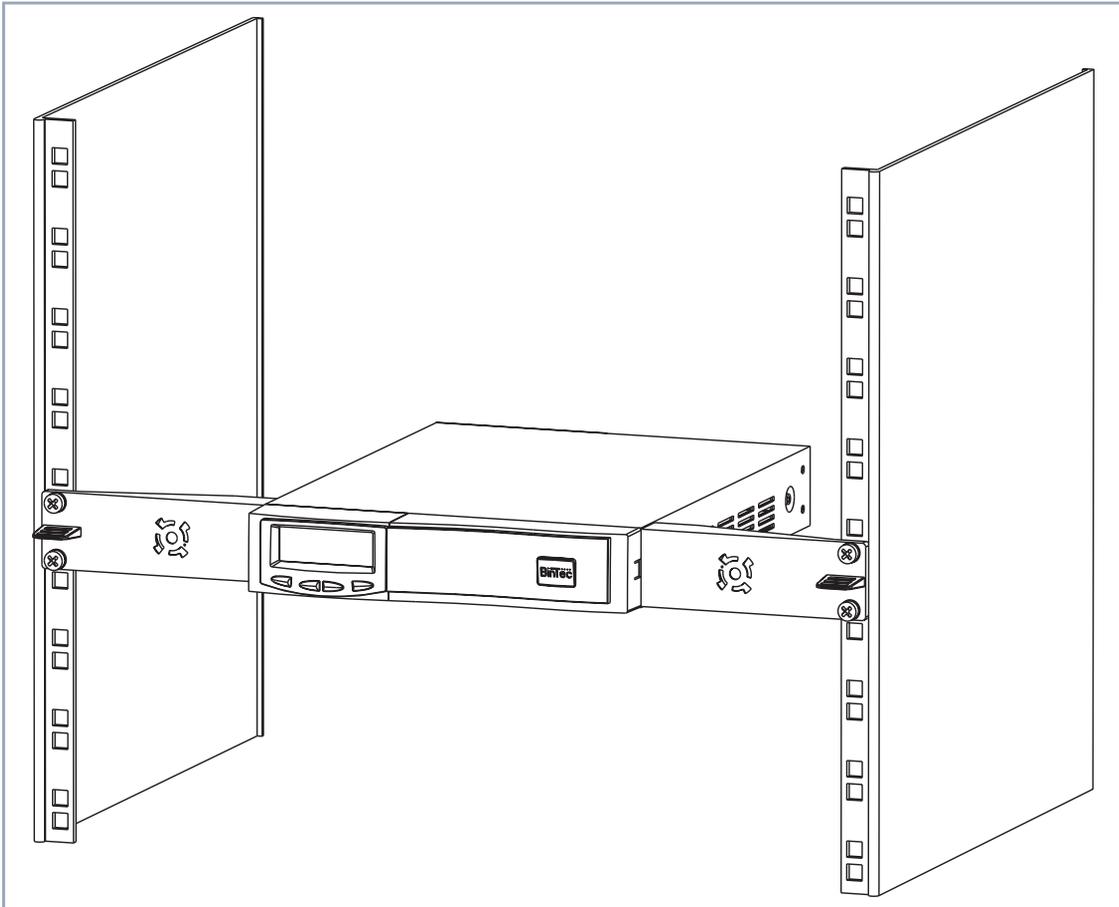


Bild 3-6: **X4000** fertig montiert im 19-Zoll-Schrank

Zum Anschließen Ihres 19-Zoll-Einbaugeräts gehen Sie zu [Kapitel 3.3, Seite 59](#).

**Ausbau aus einem
19-Zoll-Schrank**

Zum Ausbau von **X4000** 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.

Einbau mit Anschlüssen nach vorne und Umstecken des Displays



Achtung!

Zum Anschließen, Betreiben und auch zum Ein- bzw. Ausbau der Erweiterungskarte ist das Öffnen des Gehäuses nicht erforderlich.

Falls das Gehäuse dennoch geöffnet wird, reißt das Garantielabel an **X4000** und damit erlischt die Garantie.

➤ Öffnen Sie keinesfalls das Gehäuse!



Gefahr!

Beim geöffnetem Gerät sind netzspannungsführende Bauteile zugänglich. Es besteht Lebensgefahr!

➤ Öffnen Sie keinesfalls das Gehäuse!



Achtung!

X4000 muß vor dem Umstecken der Display-Baugruppe ausgeschaltet werden. Bei Umstecken der Display-Baugruppe bei eingeschaltetem Gerät kann sowohl das Display als auch das Grundgerät zerstört werden.

➤ **X4000** vor dem Umstecken der Display-Baugruppe ausschalten!

Gehen Sie folgendermaßen vor:

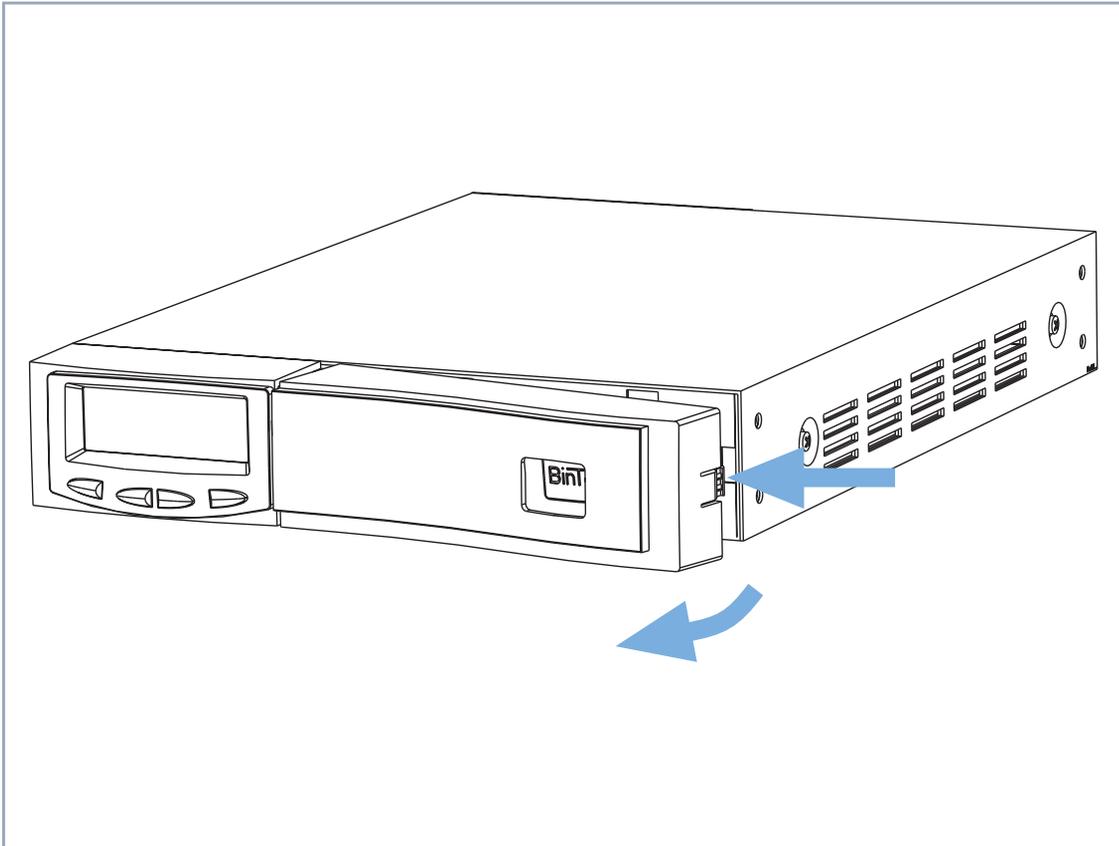


Bild 3-7: Abnehmen der Kunststoffblende

- Schritt 1** ➤ Nehmen Sie die Kunststoffblende von **X4000** vom Metallgehäuse ab. Drücken Sie dazu die mit einer Griffmarkierung versehene Schmalseite der Frontblende am Gehäuserand leicht in Richtung des Displays, siehe [Bild 3-7, Seite 46](#).

Dadurch wird die Kunststoffblende entriegelt und lässt sich nach vorne abnehmen. Die blaue Power-LED mit dem BinTec-Logo bleibt auch nach Abnehmen der Frontblende stehen.

- Schritt 2: Umstecken des Displays** ➤ Trennen Sie das Display-Verbindungskabel von der RJ11-Buchse des Metallgehäuses (Vorsicht: Stecker ist mit der Buchse verriegelt, achten Sie darauf, den Stecker zu lösen).

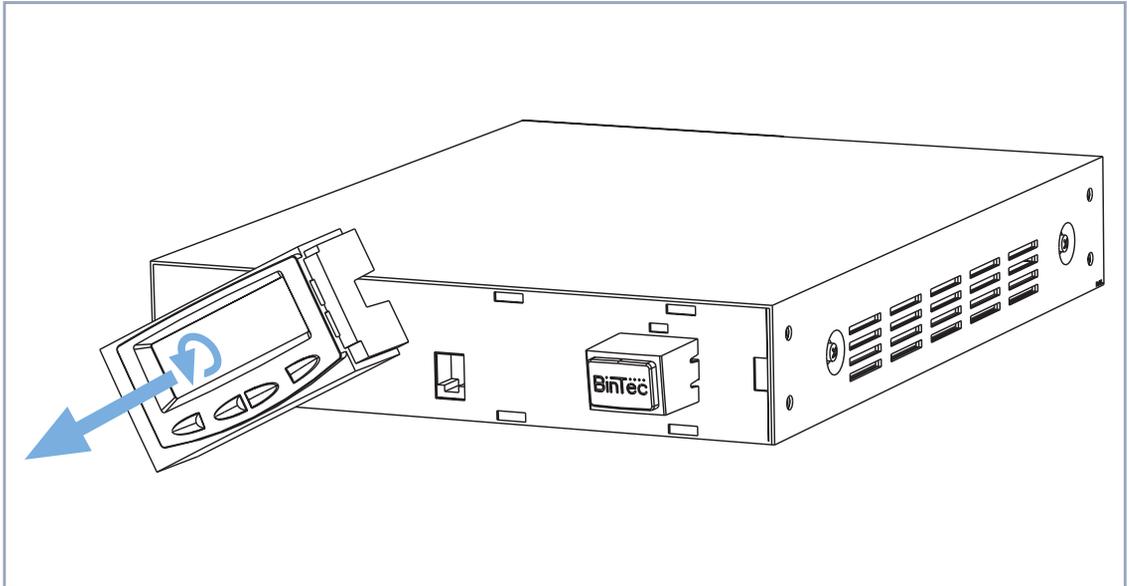
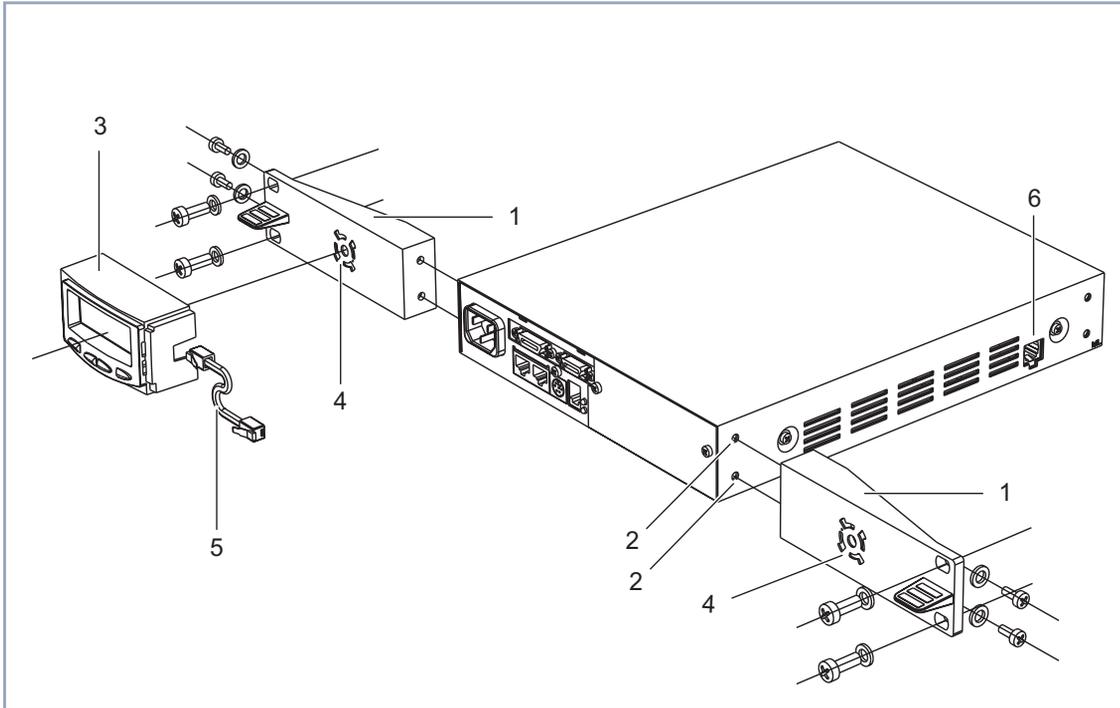


Bild 3-8: Abnehmen des Displays

- Schritt 3** ➤ Drehen Sie die Display-Baugruppe um ca. 40° nach links und ziehen Sie die Display-Baugruppe nach vorne vom Metallgehäuse weg (Bajonettverschluß), siehe [Bild 3-8, Seite 47](#).

Folgende Bau- und Befestigungsteile benötigen Sie für den Einbau in einen 19-Zoll-Schrank mit den **X4000**-Anschlüssen nach vorne:



1	Befestigungswinkel	4	Bajonettverschluß zum Befestigen der Display-Baugruppe
2	Befestigungslöcher	5	Display-Verbindungskabel
3	Display-Baugruppe	6	Stromversorgung für externe Lüfterkassette (nur bei 19-Zoll-Einbaugerät).

Bild 3-9: Explosionszeichnung mit den wichtigsten Bau- und Befestigungsteilen für den Einbau von **X4000** in einen 19-Zoll-Schrank

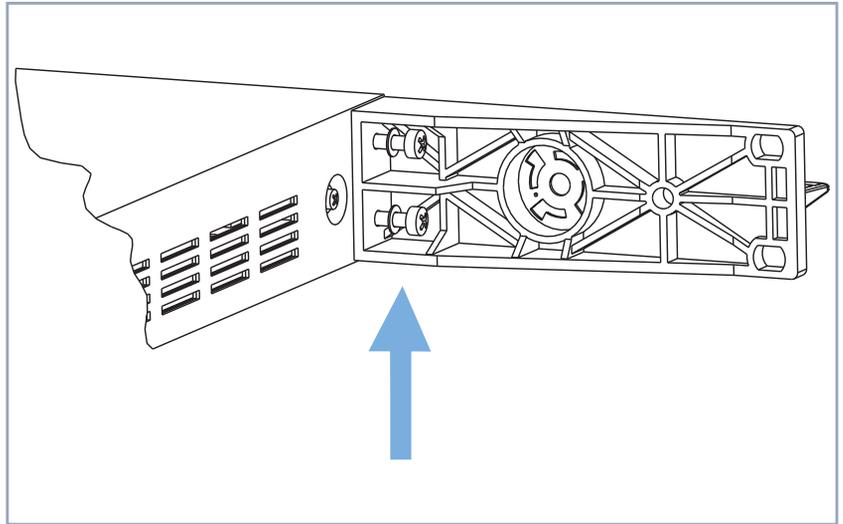


Bild 3-10: Winkel an Befestigungslöcher festschrauben

- Schritt 4** ➤ Schrauben Sie die beiden mitgelieferten Befestigungswinkel mit den mitgelieferten Schrauben an die hinteren, seitlich von **X4000** dafür vorgesehenen Befestigungslöcher fest, siehe [Bild 3-10, Seite 49](#). Verwenden Sie unbedingt die mitgelieferten Schrauben. Andere Schrauben halten den mechanischen Belastungen nicht stand oder können das Gerät zerstören.

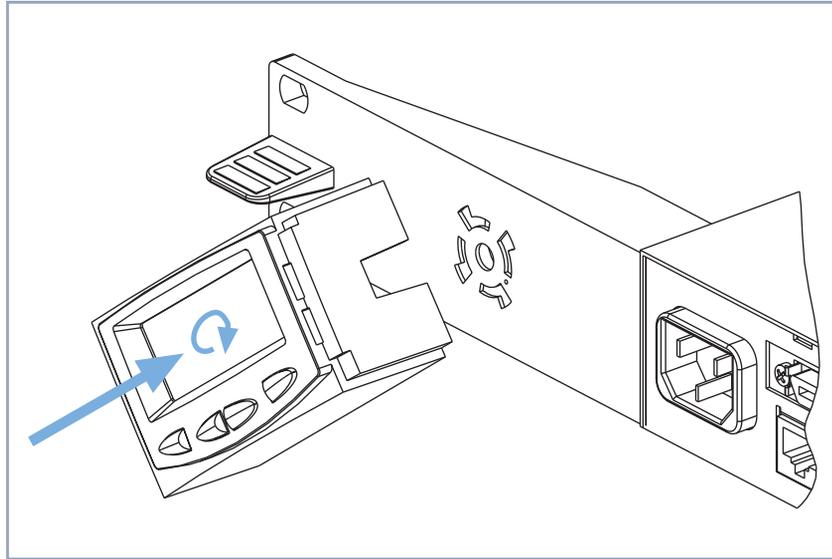


Bild 3-11: Anbau des Displays an einen Befestigungswinkel

- Schritt 5** ➤ Stecken Sie die Display-Baugruppe auf einen der beiden Befestigungswinkel. Achten Sie bitte darauf, daß die Display-Baugruppe richtig einrastet, siehe [Bild 3-12, Seite 51](#).

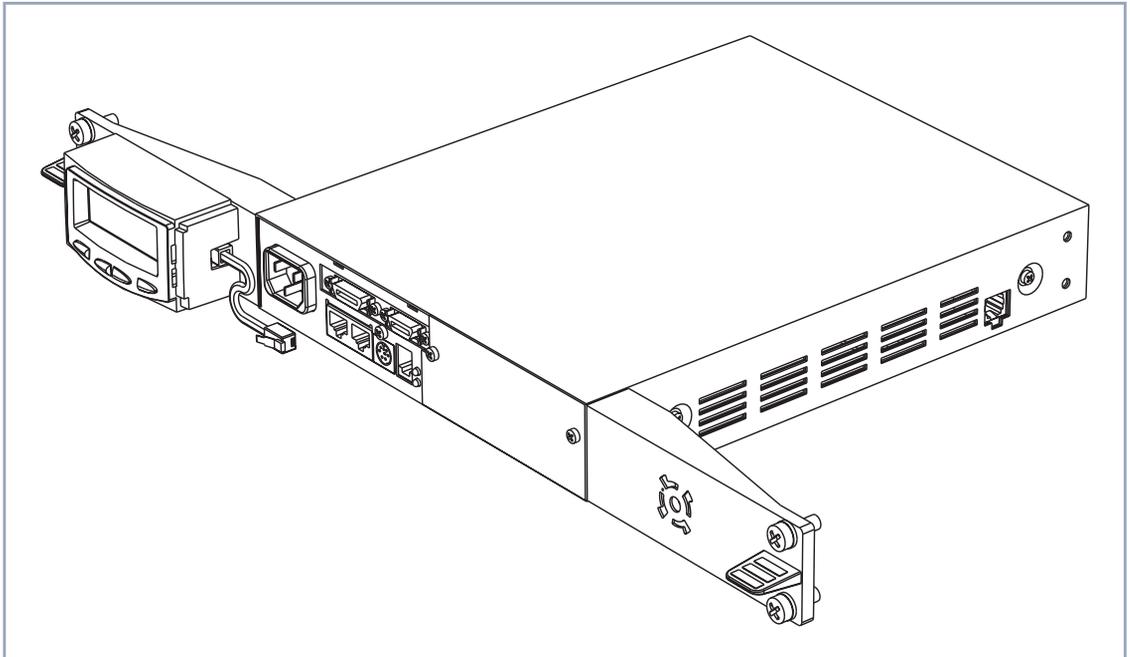


Bild 3-12: Display an einen der seitlichen Winkel anbringen

- Schritt 6** ➤ Schieben Sie diese vormontierte Einheit mit den beiden angeschraubten Winkeln in Ihren Schrank und verschrauben Sie sie mit den Längsprofilen des Schrankes (diese Schrauben sind nicht im Lieferumfang von **X4000** enthalten, sondern sind Bestandteil des Schranklieferumfangs), siehe [Bild 3-13, Seite 52](#).
- Schritt 7** ➤ Stecken Sie den Stecker des Display-Verbindungskabels in die dafür vorgesehene RJ11-Buchse.

So sollte **X4000** fertig montiert aussehen:

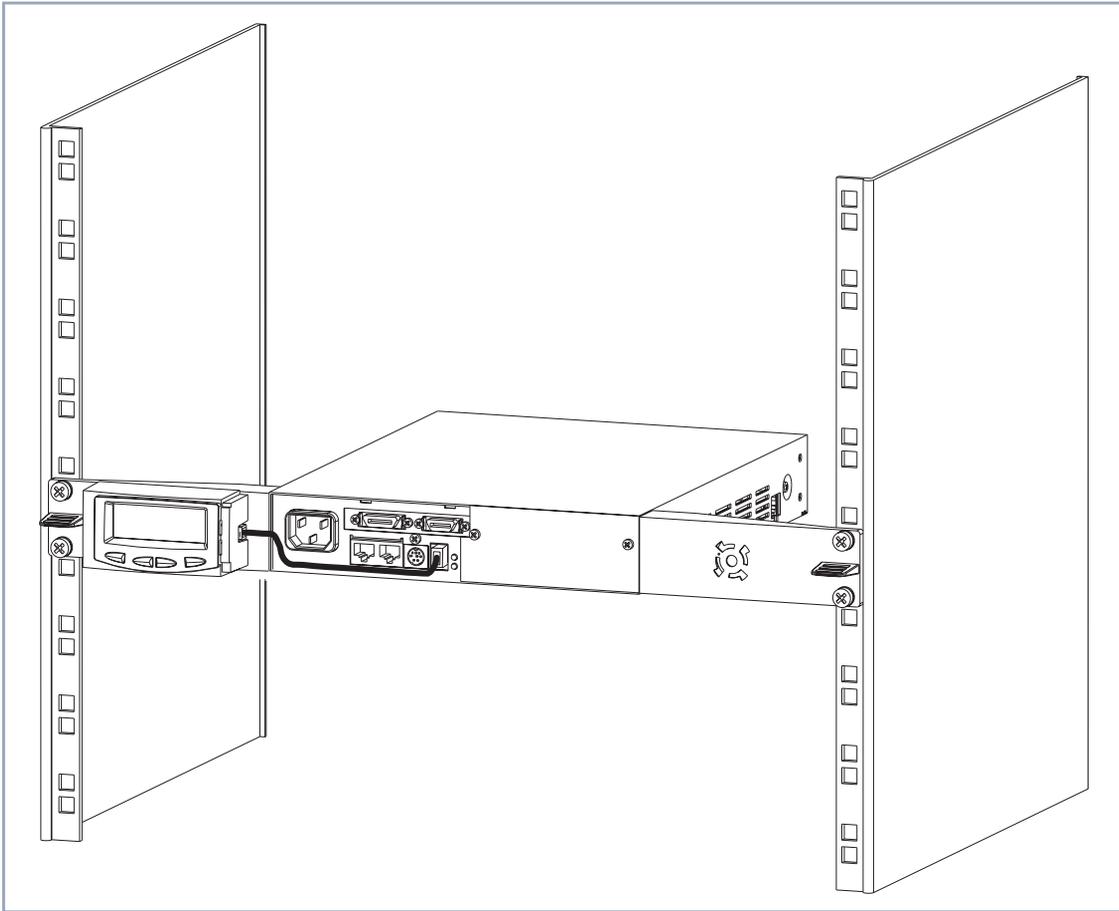


Bild 3-13: Fertig montierter **X4000** mit Anschlüssen vorne

Zum Anschließen Ihres 19-Zoll-Einbaugeräts gehen Sie zu [Kapitel 3.3, Seite 59](#).

**Ausbau aus einem
19-Zoll-Schrank**

Zum Ausbau von **X4000** aus dem 19-Zoll-Schrank (z. B. für den Einbau einer Lüfterkassette, etc.), führen Sie bitte die oben beschriebenen Schritte in umgekehrter Reihenfolge durch.

3.2 Erweiterungs- und Ressourcenkarten

Mit einer **X4000**-Erweiterungskarte können Sie Ihr Grundgerät erweitern.

Folgende Erweiterungskarten werden von BinTec für die Integration in **X4000** angeboten:

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

Zur Konfiguration der Erweiterungs- und Ressourcenkarten beachten Sie bitte [Kapitel 9, Seite 287](#). Die technischen Daten (einschließlich Pinbelegung der Schnittstellen) finden Sie in [Kapitel 13.3, Seite 422](#).

3.2.1 Ausführung der Erweiterungskarten

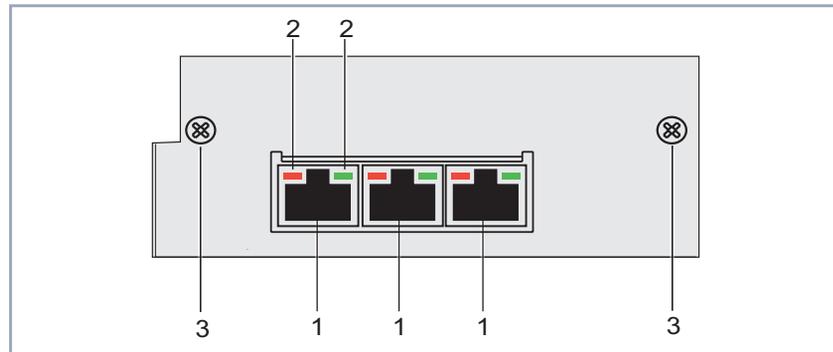
Im folgenden werden die Rückansichten der Erweiterungskarten mit den jeweils verfügbaren Schnittstellen und LEDs dargestellt.

Die Bedeutung der LEDs finden Sie in [Kapitel 3.4.2, Seite 64](#).



Bei Verwendung einer Erweiterungskarte mit Ressourcenkarte(n) im **X4000**-Einbaugerät empfiehlt BinTec Communications AG die Verwendung der optional erhältlichen Lüfterkassette.

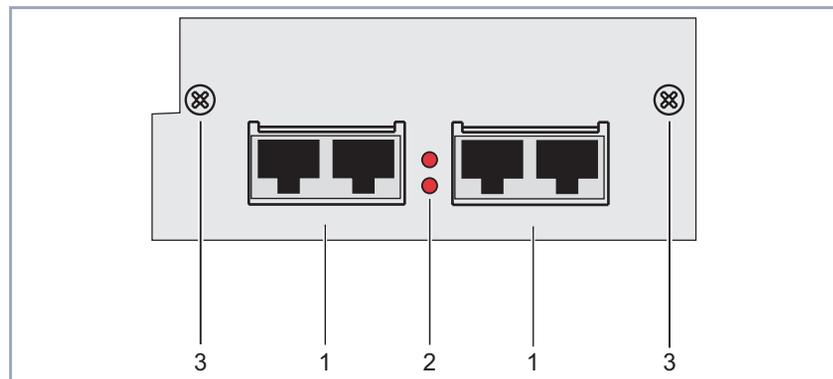
BRI-Erweiterungskarte X4E-2/3BRI



1	ISDN-BRI-Port	2	LEDs
3	Befestigungsschrauben		

Bild 3-14: Rückansicht einer BRI-Erweiterungskarte

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



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

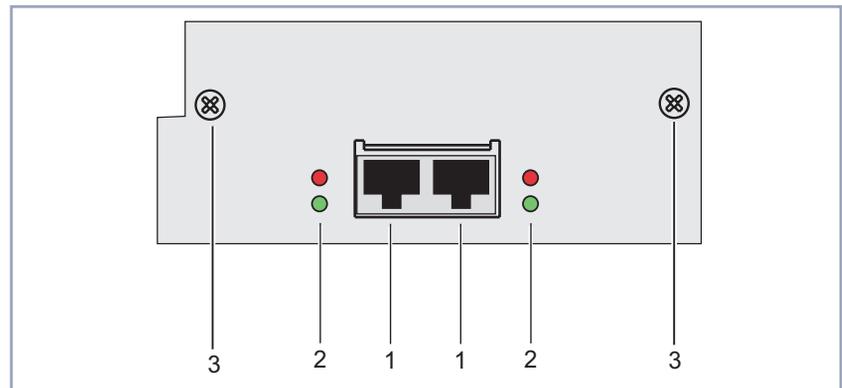
Bild 3-15: Rückansicht einer PRI-/G.703-Erweiterungskarte

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.

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



1	Fast-Ethernet-Port	2	LEDs
3	Befestigungsschrauben		

Bild 3-16: Rückansicht einer LAN-Erweiterungskarte

3.2.2 Einbau und Austausch der Erweiterungskarte

An dieser Stelle erfahren Sie, wie Sie das **X4000**-Grundgerät mit einer Erweiterungskarte bestücken oder diese gegen eine der anderen **X4000**-Erweiterungskarten austauschen können. Beachten Sie bitte auch unbedingt die im

Lieferumfang der Erweiterungs- und Ressourcenkarten enthaltene Einbauleitung!



Achtung!

Der Einbau oder Austausch einer Erweiterungskarte darf nicht im laufenden Betrieb durchgeführt werden. **X4000** muß auf jeden Fall von der Stromversorgung getrennt werden, sonst besteht die Gefahr, daß sowohl **X4000** als auch die Erweiterungskarte zerstört werden.

- Ziehen Sie immer den Netzstecker von **X4000** und alle Verbindungsleitungen der Erweiterungskarte, bevor Sie die Erweiterungskarte einstecken oder austauschen.
- Schließen Sie **X4000** 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!

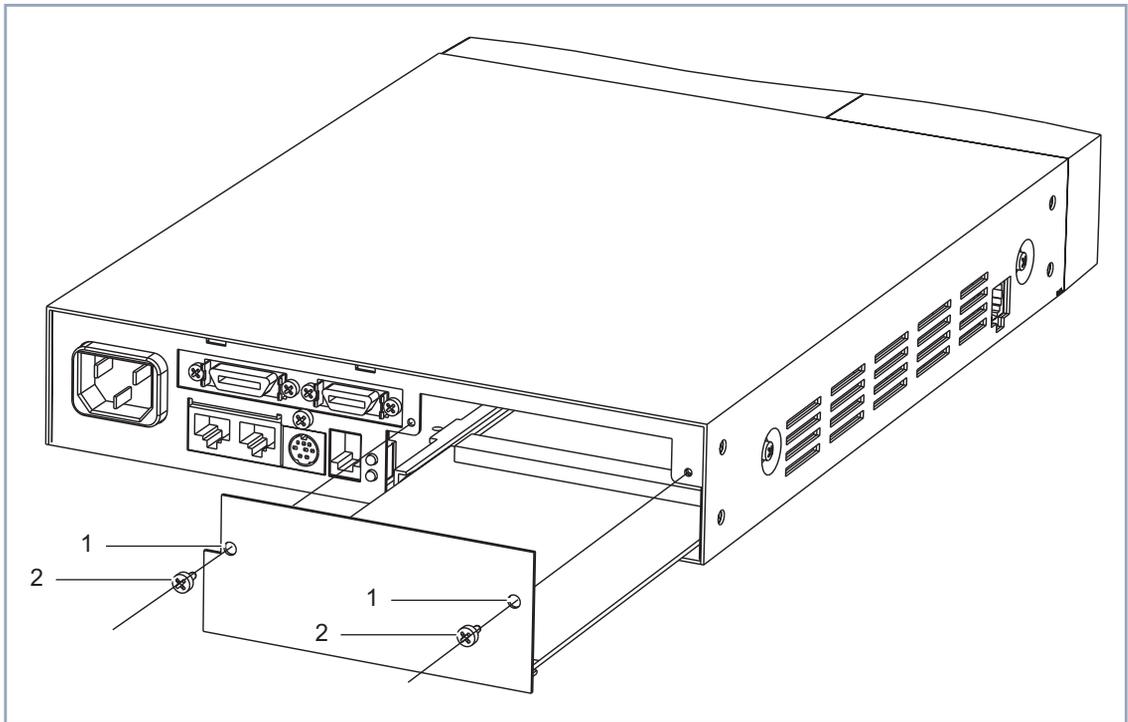
- Fassen Sie nicht in den Erweiterungssteckplatz von **X4000**!



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 Bauteile immer nur an den Rändern der Platinen, und fassen Sie nicht auf Leitungen oder Bauteile.



1, 2	Bohrung und Schraube zum Befestigen der Erweiterungskarte
------	---

Bild 3-17: Installation einer Erweiterungskarte

Einbau / Austausch

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

- 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.

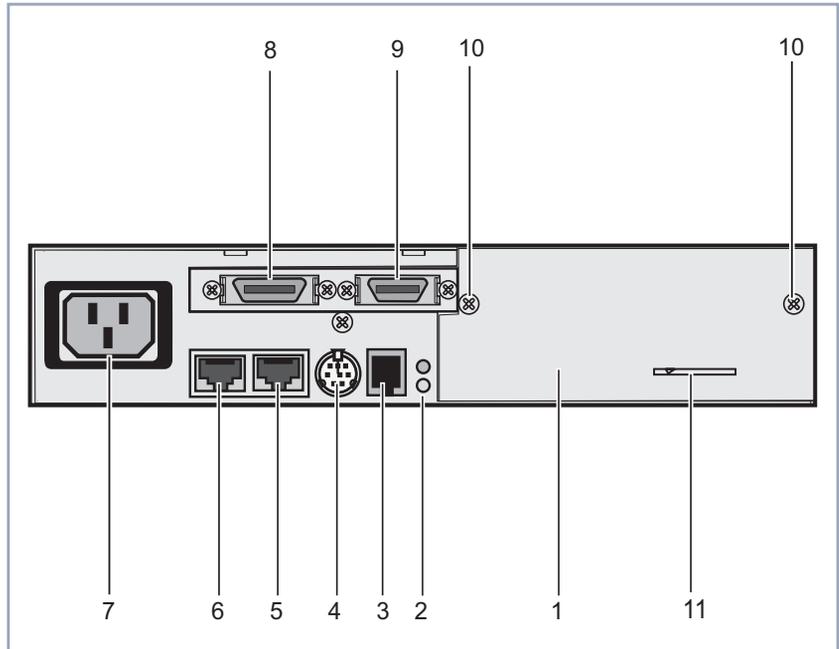
- Stecken Sie die einzubauende Erweiterungskarte in den dafür vorgesehenen Steckplatz des Gehäuses, bis sie in den Steckverbinder des Steckplatzes eingerastet ist. Kartenführungen ermöglichen ein sicheres Stecken der Erweiterungskarte. Nachdem die Erweiterungskarte eingerastet ist, befestigen Sie sie mit den beiden Schrauben, die Sie zuvor von der Blindabdeckung gelöst oder von der auszutauschenden Erweiterungskarte behalten haben (siehe [Bild 3-17](#), [Seite 57](#)), am Gehäuse.



Bei Verwendung einer Erweiterungskarten mit Ressourcenkarte(n) im **X4000**-Einbaugerät empfiehlt BinTec Communications AG die Verwendung der optional erhältlichen Lüfterkassette.

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

3.3 Aufstellen und Anschließen



1	Erweiterungskartensteckplatz (mit Blindabdeckung)	7	Kaltgerätebuchse des Netzteils
2	Status-LEDs (rot und grün)	8	X.21/V.35/V.36-Schnittstelle
3	RJ11-Buchse für Display	9	X.21bis-Schnittstelle
4	Mini-DIN-Buchse (Konsole)	10	Befestigungsschrauben der Erweiterungskarte bzw. der Blindabdeckung
5	Ethernet/LAN-Schnittstelle 10/100 Base-T-Fast Ethernet	11	Kunststoffstreifen zum Aktivieren der Pufferbatterie für die Real-Time-Clock (RTC)
6	ISDN-BRI-Schnittstelle		

Bild 3-18: **X4000**-Rückansicht



Achtung!

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

- Verbinden Sie immer nur die LAN-Schnittstelle von **X4000** mit der LAN-Schnittstelle des Hubs und die ISDN-Schnittstelle von **X4000** mit dem ISDN-Anschluß.

Gehen Sie beim Anschließen in folgender Reihenfolge vor:

- Stellen Sie **X4000** auf eine feste, ebene Unterlage.
- Verbinden Sie die serielle Schnittstelle Ihres Rechners (COM1 oder COM2) mit der Konsolenschnittstelle von **X4000**. Verwenden Sie dazu das mitgelieferte serielle Kabel.
Das Anschließen von **X4000** an die Konsolenschnittstelle (Nr. 4, siehe [Bild 3-18, Seite 59](#)) ist nur dann erforderlich, wenn Sie Ihre Initialkonfiguration über den Konsolenport seriell vornehmen möchten, z. B. mit dem Configuration Wizard (vgl. [Kapitel 6, Seite 109](#)).

X4000 an PC oder Terminal anschließen



Wenn Sie **X4000** nur schnell die IP-Adresse und Netzmaske zuweisen wollen, ist keine serielle Verbindung erforderlich. Das Zuweisen der IP-Adresse können Sie schnell und einfach mit den Eingabetasten und dem Display erledigen (vgl. [Kapitel 5, Seite 93](#)).

X4000 an LAN anschließen

- Verbinden Sie die LAN-Schnittstelle (Nr. 5, siehe [Bild 3-18, Seite 59](#)) **X4000** mit Ihrem Hub. Verwenden Sie dazu nur CAT5-taugliche LAN-Kabel. Eine schlechtere Kabelqualität kann zu Fehlfunktionen von **X4000** führen.

X4000 an WAN anschließen

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

- Verbinden Sie die ISDN-BRI-Schnittstelle (Nr. 6, siehe [Bild 3-18, Seite 59](#)) von **X4000** über das mitgelieferte Kabel (RJ-45) mit Ihrem ISDN-Anschluß.

Wenn Sie in Ihrem Anwendungsszenario die X.21/V.35/V.36- bzw. X.21bis-Schnittstelle(n) verwenden wollen:

- Verbinden Sie die X.21/V.35/V.36- Schnittstelle bzw. X.21bis-Schnittstelle (Nr. 8 bzw. Nr. 9, [Bild 3-18, Seite 59](#)) von **X4000** 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!

Real-Time-Clock Schließlich müssen Sie die Pufferbatterie der Real-Time-Clock aktivieren:

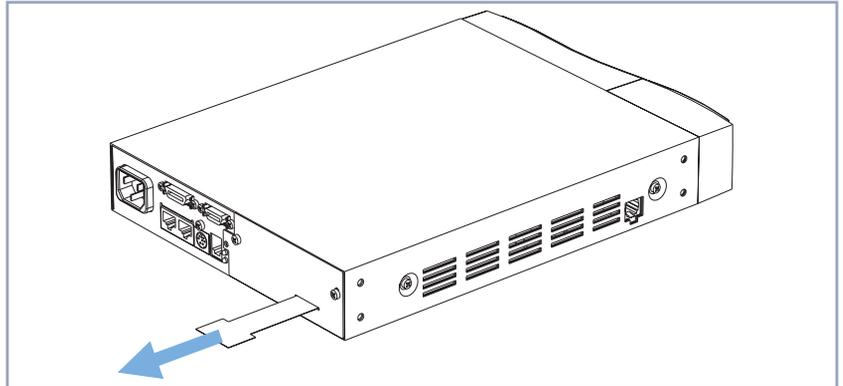


Bild 3-19: Entfernen des Kunststoffstreifens zum Aktivieren der Pufferbatterie

- Ziehen Sie den Kunststoffstreifen (siehe [Bild 3-19, Seite 61](#)) aus der Blindabdeckung.

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.

X4000 an die Stromversorgung anschließen

- Stellen Sie beim 19-Zoll-Einbaugerät sicher, daß sich das Display-Kabel in der dafür vorgesehenen Buchse befindet, sofern Sie das Display nutzen wollen.

- Schließen Sie **X4000** über das mitgelieferte Kaltgerätenetzkabel an eine Steckdose bzw. an die Stromversorgung des 19-Zoll-Schranks an.

X4000-Selbsttest

X4000 führt einen Selbsttest durch, siehe auch [Kapitel 3.5, Seite 66](#). 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 von **X4000**.

Die blaue Power-LED leuchtet, solange **X4000** mit Strom versorgt wird.



Die Statusmeldungen, die über Leuchtdioden (LEDs) angezeigt werden, finden Sie in [Kapitel 3.4, Seite 63](#).

Hardware-Grundeinstellungen

- Nehmen Sie über Tastatur und Display die erforderlichen Hardware-Grundeinstellungen vor (eine detaillierte Beschreibung finden Sie in [Kapitel 5, Seite 93](#)):
 - Dialogsprache im MMI auswählen.
 - IP-Adresse und Netzmaske eingeben, damit die weitere Konfiguration über das LAN erfolgen kann und nicht mehr über den Konsolenport durchgeführt werden muß.

3.4 Statusmeldung über Leuchtdioden (LEDs)

Im folgenden werden die drei verschiedenen LED-Arten vorgestellt, über die das **X4000**-Grundgerät Statusmeldungen abgeben kann, und die Bedeutung der LEDs auf den Erweiterungskarten.

3.4.1 Grundgerät

Power-LED Die blaue Power-LED innerhalb des BinTec-Logos auf der Vorderseite von **X4000** (siehe [Bild 3-1, Seite 37](#)) leuchtet, sobald **X4000** mit Strom versorgt wird.

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

Taste	An	Blinkt	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 3-1: Statusmeldung über Eingabetasten

LEDs auf der Rückseite von X4000 Über jeweils eine rote und eine grüne LED auf der Rückseite des **X4000**-Grundgeräts (siehe [Bild 3-2, Seite 39](#)) wird der generelle Status der einzelnen Schnittstellen angezeigt.

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.

3.4.2 Erweiterungskarten

Die Erweiterungskarten sind mit Leuchtdioden ausgestattet, die bei gesteckten Anschlußkabeln folgendermaßen reagieren.

BRI-Erweiterungskarte X4E-2/3BRI

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

Die LEDs 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
rote LED	X		D-Kanal fehlt oder Autokonfiguration schlug fehl
		X	Schicht 1 nicht stabil

Tabelle 3-2: 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 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 <i>G.703</i> ausgewählt)
–	X	Port befindet sich im PRI-Modus (Lizenz für PRI ist aktiviert und unter ISDN Line Framing ist nicht <i>G.703</i> ausgewählt)

Tabelle 3-3: 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 leuchten bei Ethernet-Collisionen 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 3-4: Statusmeldungen der LEDs einer LAN-Erweiterungskarte

3.5 Boot-Sequenz

Beim Hochfahren von **X4000** werden verschiedene Funktionszustände durchlaufen:

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

Nachdem im Start-Modus einige Selbsttests erfolgreich ausgeführt wurden, erreicht **X4000** den BOOTmonitor-Modus. Der BOOTmonitor-Prompt wird angezeigt, falls Sie über ein Terminalprogramm mit **X4000** 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 **X4000** 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:
X4000 lädt die komprimierte Boot-Datei vom Flash-Speicher in den Arbeitsspeicher. Dies wird beim Hochfahren automatisch ausgeführt.
- (2) Software Update via TFTP:
X4000 führt ein Software-Update über einen TFTP-Server aus.
- (3) Software Update via XMODEM:
X4000 führt ein Software-Update über eine serielle Schnittstelle mit XMODEM aus.
- (4) Delete Configuration:
X4000 wird in den Auslieferungszustand zurückversetzt. Alle Konfigurationsdateien werden gelöscht, die BOOTmonitor-Einstellungen werden auf die Standardwerte gesetzt.

■ (5) Default BOOTmonitor Parameters:

Sie können die Standard-Einstellungen von **X4000s** BOOTmonitor verändern, z. B. die Baudrate für serielle Verbindungen.



Wenn Sie die Baudrate verändern (voreingestellt ist 9600 Baud), achten Sie darauf, daß das verwendete Terminalprogramm diese Baudrate verwendet. Wenn dies nicht der Fall ist, können Sie keine serielle Verbindung zu **X4000** herstellen!

4 Voraussetzungen für die Konfiguration

In diesem Kapitel erfahren Sie,

- wie Sie auf **X4000** zugreifen ([Kapitel 4.1, Seite 70](#))
- wie Sie sich auf X4000 anmelden ([Kapitel 4.2, Seite 76](#))
- welche Konfigurationsmöglichkeiten Ihnen zur Verfügung stehen ([Kapitel 4.3, Seite 78](#))
- wie das ►► **Setup Tool** aufgebaut ist ([Kapitel 4.3.2, Seite 80](#))
- wie Sie bei einer Initialkonfiguration von **X4000** vorgehen sollten ([Kapitel 4.4, Seite 91](#))

4.1 Zugangsmöglichkeiten

Um **X4000** konfigurieren zu können, müssen Sie auf **X4000** zugreifen. Dafür gibt es verschiedene Möglichkeiten:

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

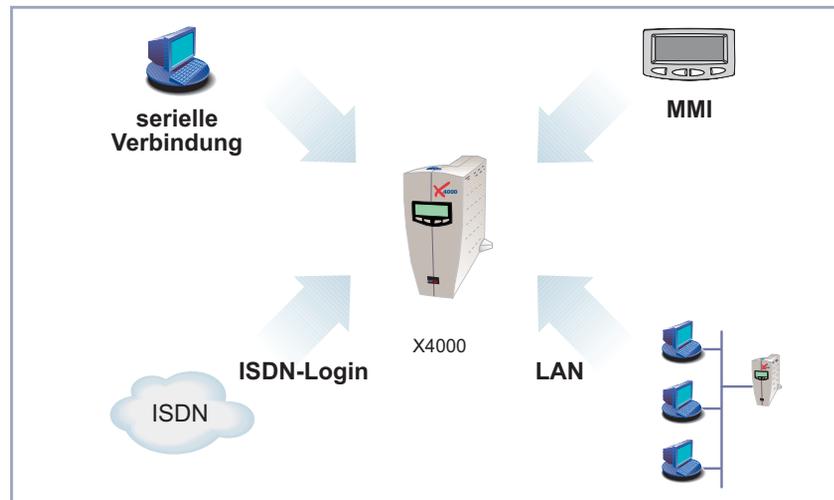


Bild 4-1: Zugangsmöglichkeiten zu **X4000**

Im folgenden werden die verschiedenen Zugangsmöglichkeiten vorgestellt. Daraus können Sie das für Ihre Bedürfnisse geeignete Vorgehen auswählen.

4.1.1 Man Machine Interface (MMI)

Erste Schritte Das MMI mit Display und Eingabetasten ist eine gute Möglichkeit, um einen "ersten Kontakt" zu **X4000** herzustellen. Mit dem MMI sollten Sie folgende erste Schritte durchführen:

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

Die weiteren Konfigurationsschritte führen Sie dann mit dem Configuration Wizard oder 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 **X4000** eine Initialkonfiguration durchführen und noch keine IP-Adresse und Netzmaske eingetragen haben. Um **X4000** über die serielle Schnittstelle an Ihren Rechner anzuschließen, verbinden Sie die serielle Schnittstelle am Grundgerät der **X4000** 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 6.2, Seite 113](#).

- ToDo**
- Klicken Sie im Windows-Startmenü auf **Programme** ➤ **BRICKware** ➤ **BRICK at COM1** (bzw. **BRICK at COM2**, wenn Sie die COM2-Schnittstelle des Rechners benutzen), um **HyperTerminal** zu starten.
 - Drücken Sie die **Eingabetaste** (evtl. mehrmals), wenn sich das **HyperTerminal**-Fenster geöffnet hat.
Es erscheint ein Fenster mit dem Login-Prompt. Sie befinden sich auf der SNMP-Shell von **X4000**.
 - Fahren Sie fort mit [Kapitel 4.2, Seite 76](#).



Falls der Login-Prompt auch nach mehrmaligem Betätigen der **Eingabetaste** nicht erscheint, konnte die Verbindung zu **X4000** 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 **X4000** 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.

Bei der Konfiguration mit dem Configuration Wizard greifen Sie ebenfalls über die serielle Schnittstelle auf **X4000** zu, aber Sie gelangen nicht auf die SNMP-Shell, sondern es erscheint das Startfenster des Configuration Wizard (siehe [Bild 6-1, Seite 114](#)).

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

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 **X4000** vom LAN aus erreichen. Telnet steht normalerweise auf jedem Rechner zur Verfügung. Um **X4000** über das LAN erreichen zu können, sollte sie bereits eine **IP-Adresse** und **Netzmaske** haben. Wenn dies nicht der Fall ist, **X4000** also noch unkonfiguriert ist, haben Sie zwei Möglichkeiten:

- Geben Sie IP-Adresse und Netzmaske über die Eingabetasten des MMI ein (siehe [Kapitel 5, Seite 93](#)).
- Wenn Sie mit Windows arbeiten, können Sie **X4000** 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 Kap. [Kapitel 6.2, Seite 113](#) beschrieben.

ToDo ➤ Schließen Sie **X4000** an das LAN an.

IP-Adresse zuweisen Gehen Sie folgendermaßen vor, um **X4000** 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 standardmäßig gestartet ist, müssen Sie ihn starten.
Nach kurzer Zeit erscheint das BootP-Server-Fenster, wenn **X4000** noch unkonfiguriert ist.
- Geben Sie in dem Fenster unter **BRICK Parameter Name** und IP Adresse von **X4000** ein.
- Klicken Sie auf **OK**.
- Schließen Sie **DIME Tools**.

Telnet ausführen Bauen Sie nun mit Telnet eine Verbindung zu **X4000** auf:

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

- Geben Sie `telnet <IP-Adresse von X4000>` ein.
- Klicken Sie auf **OK**.

Es erscheint ein Fenster mit dem Login-Prompt. Sie befinden sich auf der SNMP-Shell von **X4000**. Fahren Sie fort mit [Kapitel 4.2, Seite 76](#).

- Unix** ➤ Geben Sie `telnet <IP-Adresse von X4000>` in ein Terminal ein.
- Es erscheint ein Fenster mit dem Login-Prompt. Sie befinden sich auf der SNMP-Shell von **X4000**. Fahren Sie fort mit [Kapitel 4.2, Seite 76](#).

4.1.4 Zugang über ISDN

Remote-Konfiguration Der Zugang über ➤➤ **ISDN** mit ➤➤ **ISDN-Login** empfiehlt sich vor allem dann, wenn **X4000** aus der Ferne (Remote-LAN in [Bild 4-2, Seite 75](#)) konfiguriert oder gewartet werden soll. Dies ist auch dann möglich, wenn **X4000** sich noch im Auslieferungszustand befindet. Der Zugang erfolgt dann mithilfe eines bereits konfigurierten BinTec-Routers oder einer ISDN-Karte im Remote-LAN unter Benutzung einer Rufnummer des ISDN-Anschlusses von **X4000** im eigenen LAN (z. B. 1234).

So kann z. B. der Administrator im Remote-LAN **X4000** konfigurieren, ohne vor Ort zu sein. **X4000** in Ihrem LAN muß lediglich mit dem ISDN-Anschluß verbunden und eingeschaltet sein.

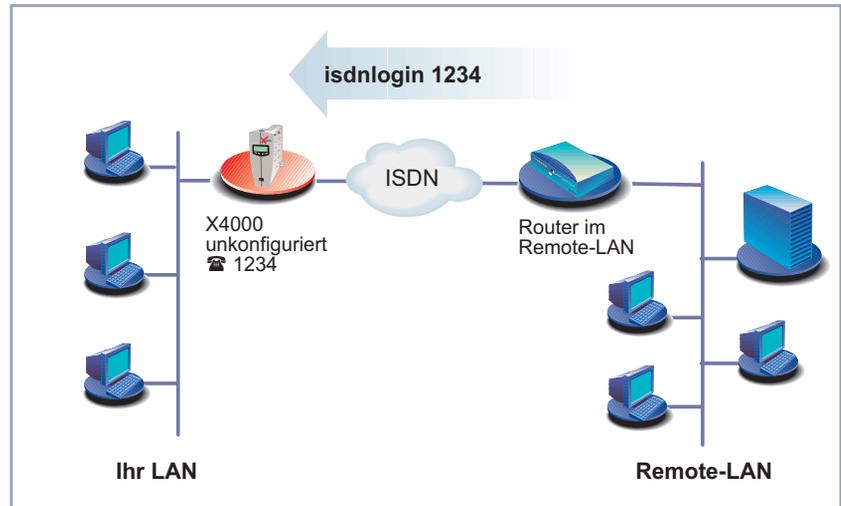


Bild 4-2: Zugang über ISDN-Login für Fernwartung



Der Zugang über ISDN verursacht Kosten. Wenn **X4000** und Rechner im gleichen LAN sind, ist es billiger, auf **X4000** über das LAN oder über die serielle Schnittstelle zuzugreifen.

ToDo ➤ Schließen Sie **X4000** an das ISDN an.

Gehen Sie folgendermaßen vor, um **X4000** über ISDN-Login zu erreichen:

- 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 X4000>` ein, z. B. `isdnlogin 1234`.

Es erscheint der Login-Prompt. Sie befinden sich auf der SNMP-Shell von **X4000**. Fahren Sie fort mit [Kapitel 4.2, Seite 76](#).

4.2 Anmelden

Unabhängig davon, über welchen Weg Sie auf **X4000** zugreifen, erscheint zunächst die **SNMP-Shell** von **X4000** mit dem Login-Prompt. Eine Ausnahme bilden hier der Configuration Wizard und der Configuration Manager unter Windows und das MMI.

Um sich anmelden zu können, müssen Sie Benutzernamen und Paßwort kennen. Im Auslieferungszustand ist **X4000** 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 X4000 verloren).
read	public	Systemvariablen lesen.
http	bintec	HTTP-Statusseite und Java-Statusmonitor von X4000 aufrufen, Systemvariablen lesen, kein Einloggen.

Tabelle 4-1: Benutzernamen und Paßwörter im Auslieferungszustand

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

Zugangsdaten (Benutzernamen und Paßwörter) sind auch nur dann änderbar, wenn sich der Benutzer `admin` einloggt. Aus Sicherheitsgründen sind Paßwörter im Setup Tool standardmäßig nicht im Klartext, sondern nur als Sternchen am Bildschirm sichtbar. Die Benutzernamen erscheinen hingegen im Klartext. Durch das Sicherheitskonzept von **X4000** 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!

Um unberechtigten Zugriff auf **X4000** zu verhindern, sollten Sie gleich als erstes die Paßwörter ändern. Die Vorgehensweise bei der Änderung von Paßwörtern ist unter "[Paßwortänderung](#)", [Seite 85](#) beschrieben.

- Ändern Sie die Paßwörter, wie in [Kapitel 7.1.2, Seite 123](#) beschrieben.

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 loslegen, müssen Sie sich für eine Methode entscheiden. Daher folgt hier zunächst eine Übersicht der verschiedenen Konfigurationsmöglichkeiten und eine Einführung in die Verwendung des Setup Tools. Anhand des Setup Tools beschreibt dieses Handbuch, wie Sie **X4000** konfigurieren.

4.3.1 Übersicht

Die Möglichkeiten, **X4000** zu konfigurieren:

- MMI (Man Machine Interface)
- Configuration Wizard
- 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 **X4000** auf dem Display anzuzeigen und einige grundlegende Einstellungen (z. B. IP-Adresse und Netzmaske) über die Eingabetasten einzugeben. Schnell und unkompliziert, ohne daß Sie sich einloggen müssen! Eine umfassende Konfiguration ist mit dem MMI nicht möglich. Dafür sollten Sie das Setup Tool oder den Configuration Wizard verwenden. Detaillierte Informationen zum MMI und die komplette Menüstruktur finden Sie in [Kapitel 5, Seite 93](#).

Configuration Wizard Die Konfiguration mit dem Configuration Wizard lernen Sie in [Kapitel 6, Seite 109](#) kennen. Sie dient zur schnellen Grundkonfiguration des **X4000**-Grundgeräts und kann genutzt werden, wenn Sie über einen Windows-PC verfügen. Standardkonfigurationen sind in der Regel damit abgedeckt. Wenn Sie aber darüberhinaus noch weitere Einstellungen benötigen bzw. wenn Sie andere WAN-Schnittstellen von **X4000** als die ISDN-BRI-Schnittstelle des Grundgerätes nutzen wollen, stehen Ihnen die anderen oben genannten Konfigurationsmöglichkeiten zur Verfügung. Sie können zunächst **X4000** mit

dem Configuration Wizard konfigurieren und anschließend die so erstellte Konfiguration mit einem der anderen Tools erweitern oder ändern. In vielen Fällen wird die Konfiguration mit dem Configuration Wizard aber ausreichend sein!

Setup Tool Das Setup Tool ist ein menügesteuertes Tool zur Konfiguration und Administration von **X4000**. Die Konfiguration mit Setup Tool ist wesentlich einfacher und übersichtlicher als die Konfiguration mit SNMP-Kommandos, allerdings können nicht alle Einstellungen mittels Setup Tool vorgenommen werden. In diesem Handbuch wird neben dem Configuration Wizard vor allem 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 Communications AG 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 **X4000** 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 **X4000** 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](#).

4.3.2 Bedienung des Setup Tools

Wenn Sie sich auf **X4000** eingeloggt haben, können Sie das Setup Tool aufrufen:

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

Das Hauptmenü des Setup Tools erscheint.

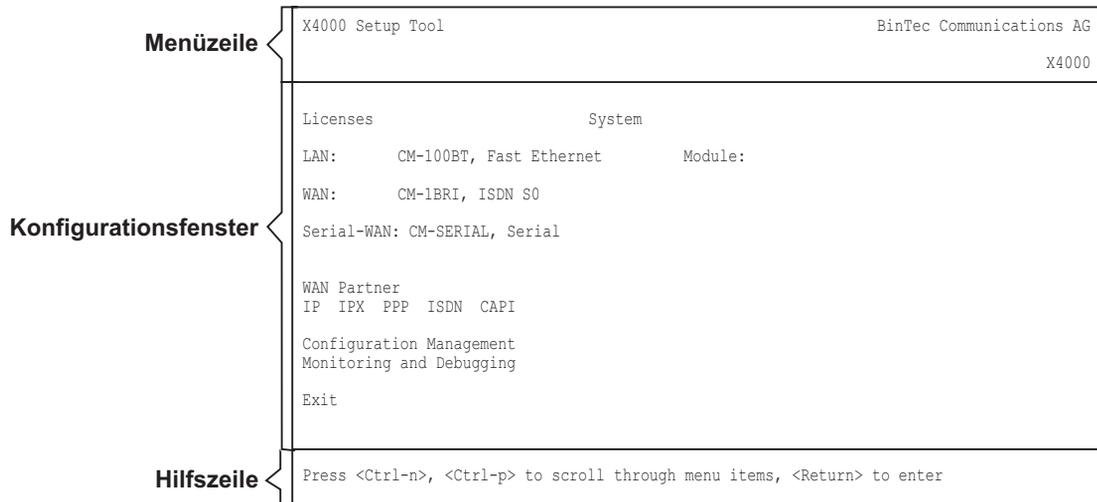


Bild 4-3: Setup Tool Menü-Layout



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 76](#)).

Das Setup Tool ist einfach zu bedienen. Nach einigen Minuten werden Sie sich gut darin zurechtfinden. Dennoch sollten Sie sich zunächst mit den Möglichkeiten des Setup Tools vertraut machen. Es folgt zunächst eine Einführung in das Setup Tool von **X4000**.

Menü-Layout Jedes Setup Tool Menü besteht aus drei Bereichen (siehe [Bild 4-3, Seite 80](#)):

In der Menüleiste befindet sich eine Navigationshilfe, die anzeigt, in welchem Menü des Setup Tools Sie sich gerade befinden. Zusätzlich wird der Systemname von **X4000** angezeigt. Dies ist insbesondere dann hilfreich, wenn Sie mehrere BinTec-Router mit unterschiedlichen Systemnamen einsetzen.

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

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

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

Tastenkombination	Bedeutung
Tabulator	Zum nächsten Feld im Menü springen.
Eingabetaste	Untermenü öffnen oder Kommando (z. B. SAVE) aktivieren.
up und down	Zum nächsten und vorherigen Feld im Menü springen (funktioniert mit VT 100-Emulation bei Verwendung eines Terminal-Programms).
left und right	Vorherige und nachfolgende Werte von Feldern sichtbar machen (funktioniert mit VT 100-Emulation bei Verwendung eines Terminal-Programms).
Esc Esc	Zweimal nacheinander Esc : Zum vorherigen Menü zurückkehren. Veränderungen gehen verloren.
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 langen Liste, die nicht vollständig angezeigt wird, nach unten blättern. Rechts unten zeigt ein "=" das Ende der Liste bzw. ein "v" weitere Listeneinträge an.
Strg - b	In einer langen Liste, die nicht vollständig angezeigt wird, nach oben blättern. Rechts oben zeigt ein "=" den Anfang der Liste bzw. ein "^" weitere Listeneinträge an.

Tastenkombination	Bedeutung
Strg - c	Setup Tool verlassen.

Tabelle 4-2: Navigation im Setup Tool

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

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

Tabelle 4-3: Schaltflächen im Setup Tool

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

```

X4000 Setup Tool                               BinTec Communications AG
[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**.



Falls die Suche nicht funktioniert, achten Sie darauf, daß sich der Cursor auf einem Listen-Element befindet.

Die Suche kann nicht ausgeführt werden, wenn sich der Cursor auf einem Kommando-Feld, z. B. **ADD** oder **DELETE**, befindet.

Beispiel:

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

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

Tabelle 4-4: Suchergebnisse

Paßwortänderung

Die im folgenden beschriebene Vorgehensweise zur Paßwortänderung betrifft alle Paßwörter auf **X4000**: die Zugangspaßwörter für die Benutzernamen **admin**, **read** und **write**, das HTTP-Paßwort, 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 **X4000** 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 **X4000** eingeloggt ist.

Um ein Paßwort zu ändern, gehen Sie folgendermaßen vor:



Im Paßwortfeld löscht die Taste **Backspace** immer die gesamte Eingabe und 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 wiederholt das neue Paßwort ein und bestätigen Sie die Eingabe mit der **Eingabetaste**, dem **Tabulator** oder einer **Cursortaste**.
Wurde das Paßwort das zweite Mal fehlerfrei eingegeben, 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 `Password doesn't match. Try again.` eingeblendet.

Menü-Struktur Das Hauptmenü des Setup Tools sieht folgendermaßen aus:

X4000 Setup Tool		BinTec Communications AG MyRouter	
Licenses	System		
LAN:	CM-100BT, Fast Ethernet	Module:	
WAN:	CM-1BRI, ISDN S0		
Serial-WAN:	CM-SERIAL, Serial		
WAN Partner			
IP	IPX	PPP	ISDN CAPI
Configuration Management			
Monitoring and Debugging			
Exit			

Die Menü-Struktur des Setup Tools sieht folgendermaßen aus:

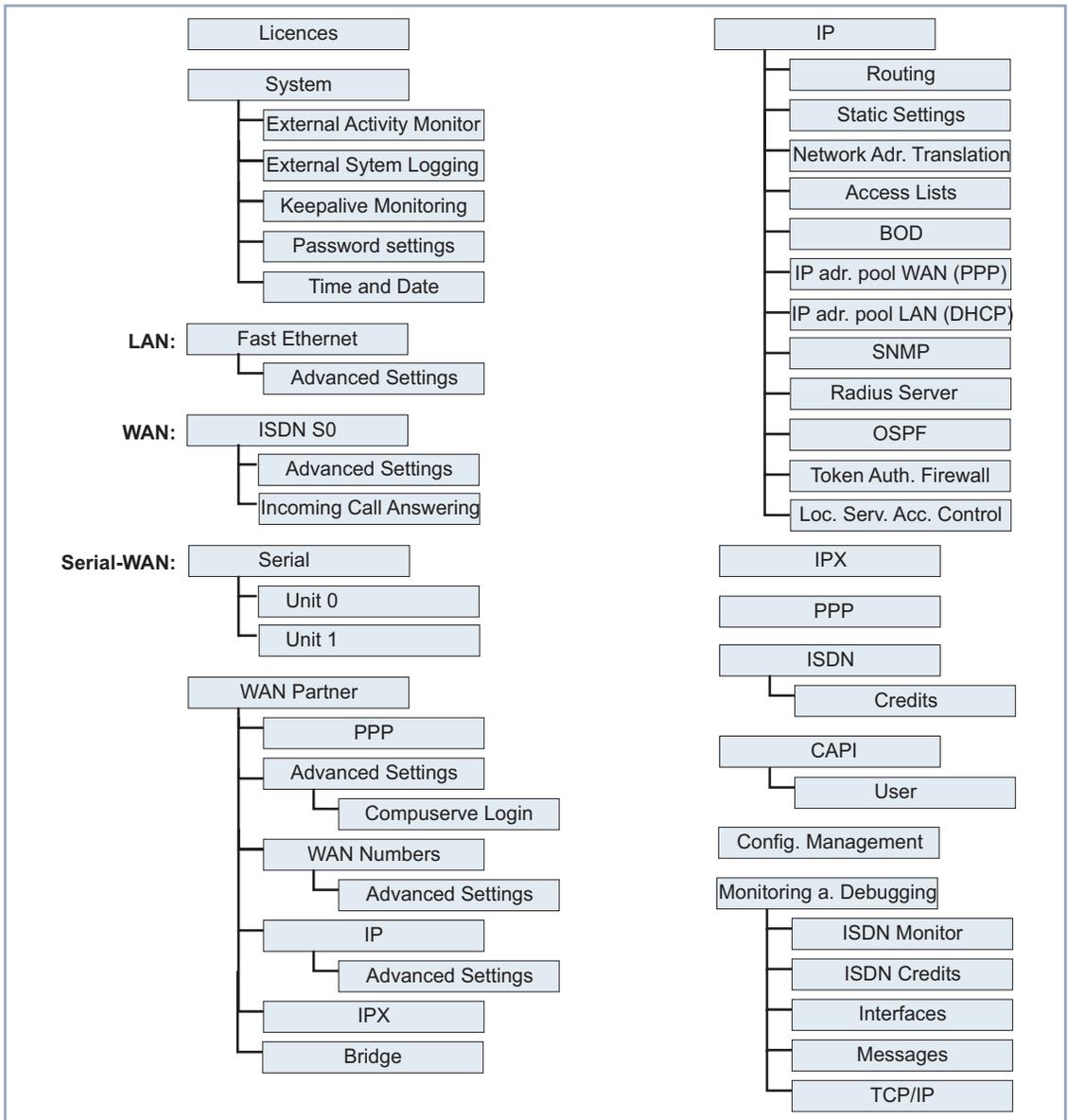


Bild 4-4: Setup Tool Menü-Struktur (Grundgerät)

Bild 4-4, Seite 87 stellt die auf **X4000** zur Verfügung stehenden Menüs des Setup Tools dar. Wenn Sie die erforderliche Lizenz aktivieren, erkennt dies **X4000** und zeigt die entsprechenden Menüs an (Lizenz eintragen siehe Kapitel 7.1.1, Seite 121).

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, die auf der mitgelieferten Lizenzkarte vermerkt sind. Hier aktivieren Sie auch die Zusatzlizenzen.
SYSTEM	In diesem Menü tragen Sie die grundlegenden Systemeinstellungen von X4000 ein, wie z. B. Systemname und Paßwörter.
FAST ETHERNET	In diesem Menü konfigurieren Sie die ►► LAN-Schnittstelle von X4000 . Hier tragen Sie z. B. die IP-Adresse und Netzmaske von X4000 ein.
ISDN S0	In diesem Menü konfigurieren Sie die ISDN-Schnittstelle von X4000 . Hier tragen Sie z. B. ein, an welcher Art von ISDN-Anschluß X4000 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.
SERIAL	In diesem Menü konfigurieren Sie die seriellen WAN-Schnittstellen von X4000 .
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	<p>In diesem Menü tragen Sie die Einstellungen ein, die das ➤➤ IP-Protokoll betreffen. Es besteht aus mehreren Untermenüs:</p> <p>IP ➤ ROUTING enthält die IP-Routing-Tabelle von X4000. Hier tragen Sie Routen zu Ihren Partnern ein (z. B. Default-Routen, Netzwerk-Routen), damit X4000 alle ➤➤ Datenpakete an die richtigen Adressen weiterleitet.</p> <p>In IP ➤ STATIC SETTINGS trage Sie einige wichtige Einstellungen ein, z. B. den Domain-Namen von X4000, die IP-Adressen zusätzlicher ➤➤ Server (z. B. Domain-Name-Server), Angaben über die Systemzeit.</p> <p>In IP ➤ NETWORK ADDRESS TRANSLATION konfigurieren Sie die Schnittstellen zu den Partnern, für die Sie die Funktion Network Address Translation (➤➤ NAT) nutzen wollen.</p> <p>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 X4000 ungewollt Verbindungen zum ISDN aufbaut.</p> <p>In IP ➤ BANDWIDTH ON DEMAND (BOD) definieren Sie Filter für die Funktion Bandwidth on Demand bzw. AO/DI (Always On/Dynamic ISDN).</p> <p>In IP ➤ IP ADDRESS POOL WAN (PPP) können Sie einen Pool von IP-Adressen einrichten, die X4000 als dynamischer IP-Address-Server an WAN-Partner vergibt, die sich einwählen.</p> <p>In IP ➤ IP ADDRESS POOL LAN (DHCP) konfigurieren Sie X4000 als ➤➤ DHCP-Server. Als DHCP-Server teilt X4000 den Hosts im LAN deren IP-Adressen dynamisch zu.</p> <p>In IP ➤ SNMP können Sie die grundlegenden ➤➤ SNMP-Einstellungen ändern.</p> <p>In IP ➤ RADIUS SERVER können Sie RADIUS-Server konfigurieren.</p> <p>In IP ➤ DNS können Sie die Vorgehensweise bei der Namensauflösung auf X4000 festlegen.</p> <p>In IP ➤ LOCAL SERVICES ACCESS CONTROL kann der Zugang zu den lokalen UDP- bzw. TCP-Diensten auf X4000 geregelt werden.</p>
IPX	<p>In diesem Menü nehmen Sie die Eintragungen vor, die das IPX-Protokoll betreffen. ➤➤ IPX wird vor allem in Novell-Netzwerken verwendet.</p>

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 X4000 .
CAPI	Enthält die Einstellungen für das ►► CAPI User Concept von BinTec. Damit können Sie an Nutzer der CAPI-Anwendungen von X4000 Benutzernamen und Paßwörter vergeben. So stellen Sie sicher, daß nur autorisierte Nutzer eingehende Rufe empfangen und ausgehende Verbindungen via CAPI aufbauen können.
CONFIGURATION MANAGEMENT	In diesem Menü verwalten Sie die Konfigurationsdateien von X4000 . Sie speichern Sie z. B. lokal auf X4000 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 X4000 , 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 X4000 wird diese Datei geladen. Mit Exit ► Exit without saving gehen seit dem letzten Hochfahren von X4000 gemachte Änderungen verloren.

Tabelle 4-5: Menüs im Setup Tool

4.4 Vorgehensweise für Initialkonfiguration

Prinzipiell empfehlen wir für die Initialkonfiguration von **X4000** folgende Vorgehensweise:

- Führen Sie die ersten Konfigurationsschritte über das MMI aus (siehe [Kapitel 5, Seite 93](#)). Dazu muß **X4000** noch nicht mit dem LAN verbunden sein, lediglich der Netzstecker muß angeschlossen sein:
 - gewünschte Display-Sprache einstellen
 - IP-Adresse und Netzmaske eintragen
- Schließen Sie **X4000** wie in [Kapitel 3.3, Seite 59](#) beschrieben an.
- Erstellen Sie eine Grundkonfiguration, wahlweise mit
 - Configuration Wizard (siehe [Kapitel 6, Seite 109](#)) oder
 - Setup Tool (siehe [Kapitel 7, Seite 119](#))
- Anschließend können Sie:
 - Weitere Funktionen mit dem Setup Tool konfigurieren (siehe [Kapitel 8, Seite 193](#)).
 - Sicherheitsfunktionen mit dem Setup Tool konfigurieren (siehe [Kapitel 10, Seite 319](#)).
 - Ihre Erweiterungskarte mit dem Setup Tool konfigurieren (siehe [Kapitel 9, Seite 287](#)).

5 Man Machine Interface (MMI) – Display mit Benutzerführung

BinTecs Man Machine Interface (MMI) mit Display und Eingabetasten erleichtert den "Ersten Kontakt" zu **X4000** und macht Statusinformationen leicht zugänglich.

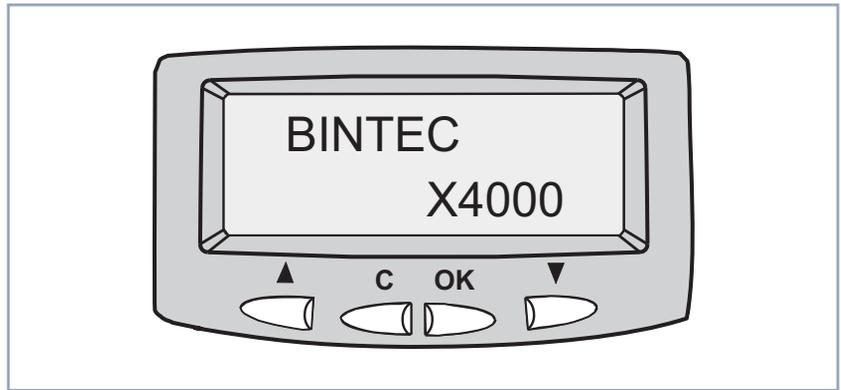


Bild 5-1: MMI mit Display und Eingabetasten (Logo)

Im diesem Kapitel finden Sie folgende Informationen:

- Einen Überblick über die Möglichkeiten des MMI ([Kapitel 5.1, Seite 94](#))
- Eine Beschreibung, wie Sie das Display und die Eingabetasten benutzen ([Kapitel 5.2, Seite 96](#))
- Eine Darstellung der Menüstruktur des MMI, hilfreich für die ersten Schritte ([Kapitel 5.3, Seite 99](#))
- Nützliche Short-Cuts ([Kapitel 5.4, Seite 107](#))

Nachdem Sie die ersten Einstellungen mit dem MMI festgelegt haben, setzen Sie die Konfiguration von **X4000** mit dem Configuration Wizard (siehe [Kapitel 6, Seite 109](#)) oder dem Setup Tool (siehe [Kapitel 7, Seite 119](#)) fort.

5.1 Überblick

Erster Kontakt Mit dem MMI können Sie IP-Adresse und Netzmaske von **X4000** eingeben, ohne vorher eine serielle Verbindung zu **X4000** herstellen zu müssen. Dies erleichtert die Initialkonfiguration. So können Sie als erstes **X4000** 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 **X4000**-Aktivitäten ermöglicht, ohne sich einloggen zu müssen. Ein zusätzliches Diagnose-Tool wird damit bereitgestellt, das z. B. den aktuellen Stand der System-Software oder die Aktivitäten der **X4000**-Schnittstellen anzeigt.

Benutzerführung Beleuchtete Eingabetasten und Navigationsleisten erleichtern die Bedienung des MMI. Damit werden Sie 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 **X4000** zunächst einige Selbsttests durch und zeigt anschließend das **X4000**-Logo auf dem Display an (siehe [Bild 5-1, Seite 93](#)). 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.



Standardmäßig wird beim Einschalten von **X4000** bzw. nach dem Ablauf des Display-Idletimers das **X4000**-Logo angezeigt.

Um dafür ein anderes MMI-Menü zu verwenden, zeigen Sie das gewünschte Menü auf dem Display an und drücken dann gleichzeitig **C** und **OK**. Nach Ablauf des Idletimers erscheint dann das entsprechende Menü statt des Logos.

So können Sie z. B. eine bestimmte Schnittstelle von **X4000** standardmäßig anzeigen und auf diese Weise überwachen.

Zugriffsschutz Standardmäßig wird das MMI im Konfigurationsmodus betrieben, 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 100](#).

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 96](#) einen Ausschnitt des Menüsystems:

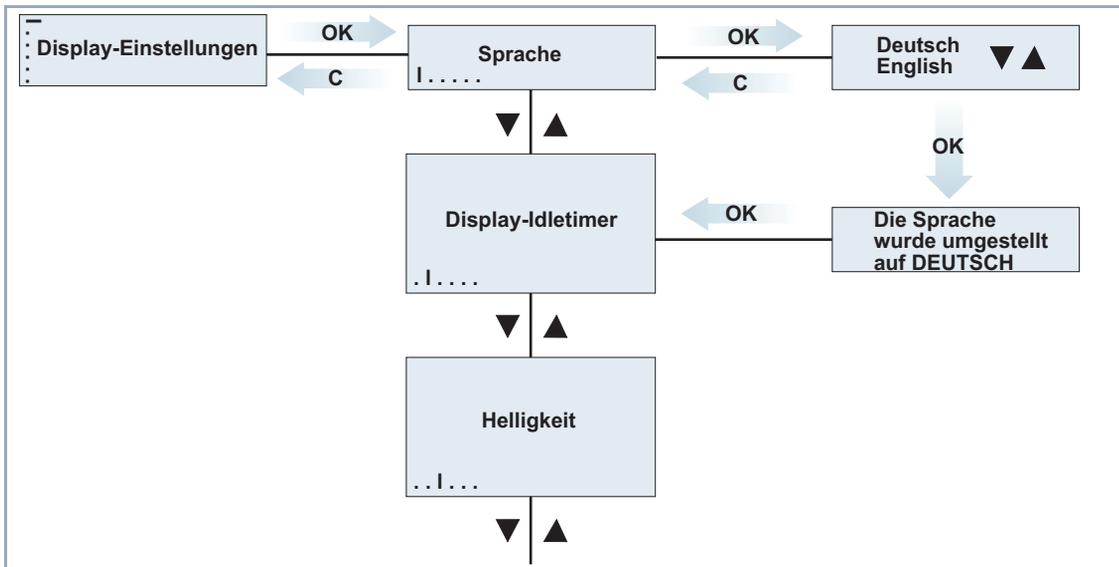


Bild 5-2: Verwenden der Eingabetasten (Ausschnitt aus Menüsystem)

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 **X4000**) 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 97](#)) und gestatten Ihnen so eine einfache und komfortable Bedienung. Nur die Tasten sind beleuchtet, die zu diesem Zeitpunkt benutzt werden können. Das Drücken der nicht-beleuchteten Tasten hat keine Auswirkung.

Taste	An	Blinkt	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

Navigationsleisten zur Orientierung

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

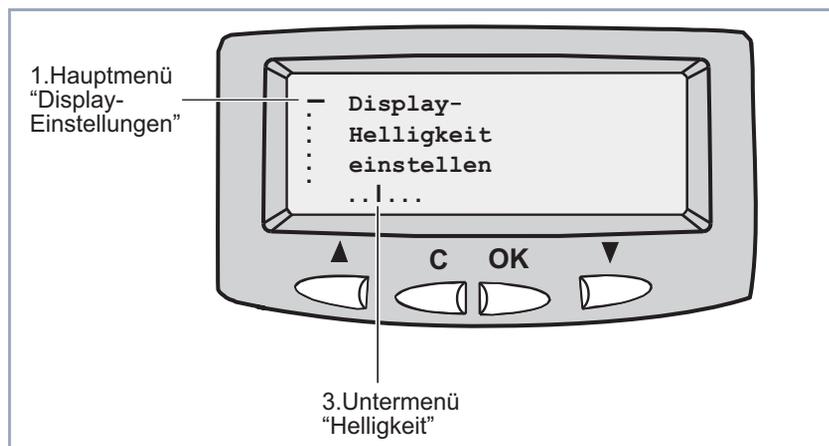


Bild 5-3: Navigationsleisten (Beispiel)

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 Sie sich innerhalb des entsprechenden Hauptmenüs befinden.

Die folgenden Abbildungen der Menüstrukturen zeigen auch die dazugehörigen Navigationsleisten.

5.3 Menüstruktur

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

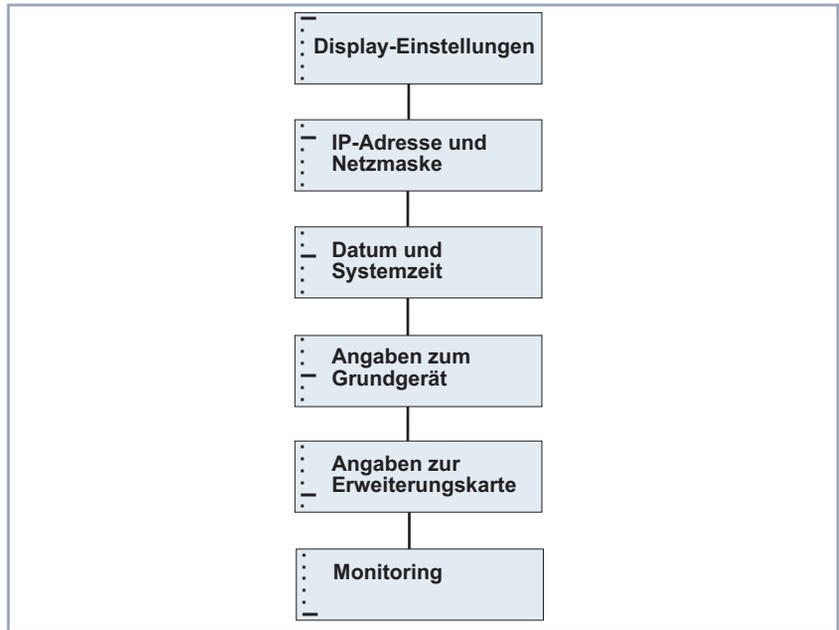


Bild 5-4: Hauptmenüs (mit Navigationsleisten)

- **Display-Einstellungen** (siehe [Kapitel 5.3.1, Seite 100](#))
- **IP-Adresse und Netzmaske** (siehe [Kapitel 5.3.2, Seite 102](#))
- **Datum und Systemzeit** (siehe [Kapitel 5.3.3, Seite 103](#))
- **Angaben zum Grundgerät** (siehe [Kapitel 5.3.4, Seite 104](#))
- **Angaben zur Erweiterungskarte** (siehe [Kapitel 5.3.5, Seite 105](#))
- **Monitoring** (siehe [Kapitel 5.3.6, Seite 106](#))



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

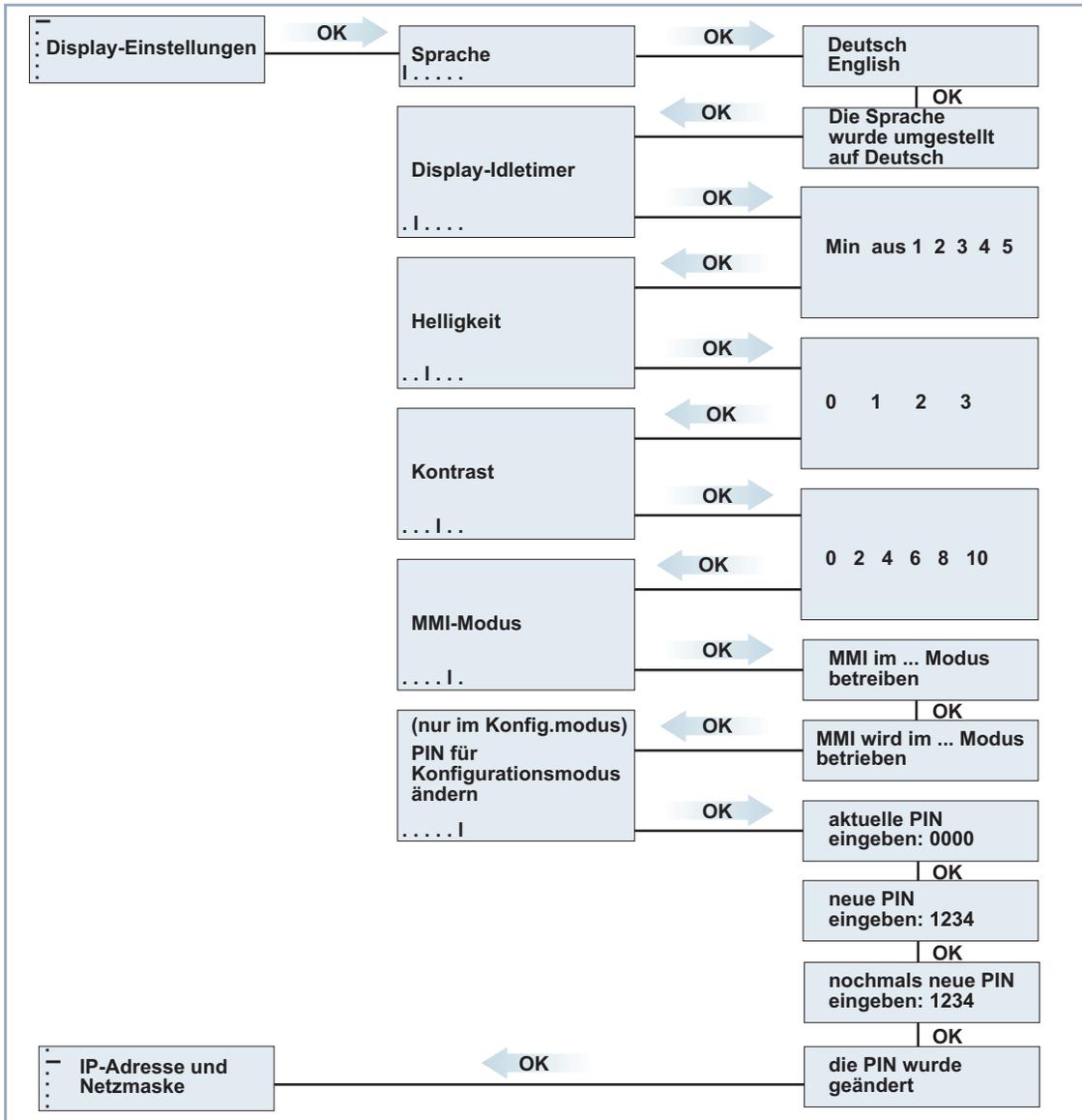


Bild 5-5: Menüs zum Auswählen der Display-Einstellungen (mit Navigationsleisten)

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 ... 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. Standardmäßig lautet die PIN im Auslieferungszustand **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:

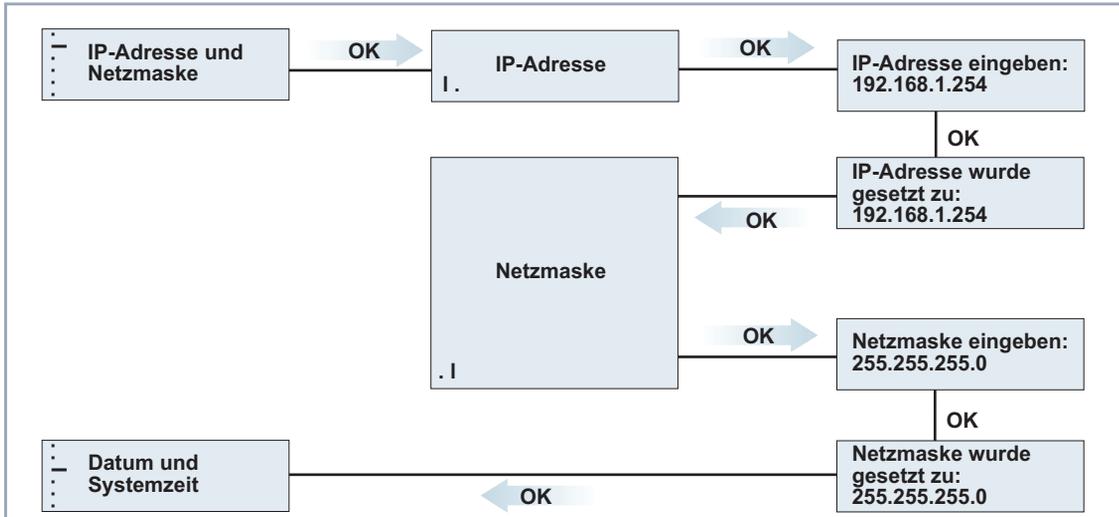


Bild 5-6: Menüs zum Eingeben von IP-Adresse/Netzmaske (mit Navigationsleisten)

■ IP-Adresse

Hier geben Sie die IP-Adresse von **X4000** 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 **X4000** 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:

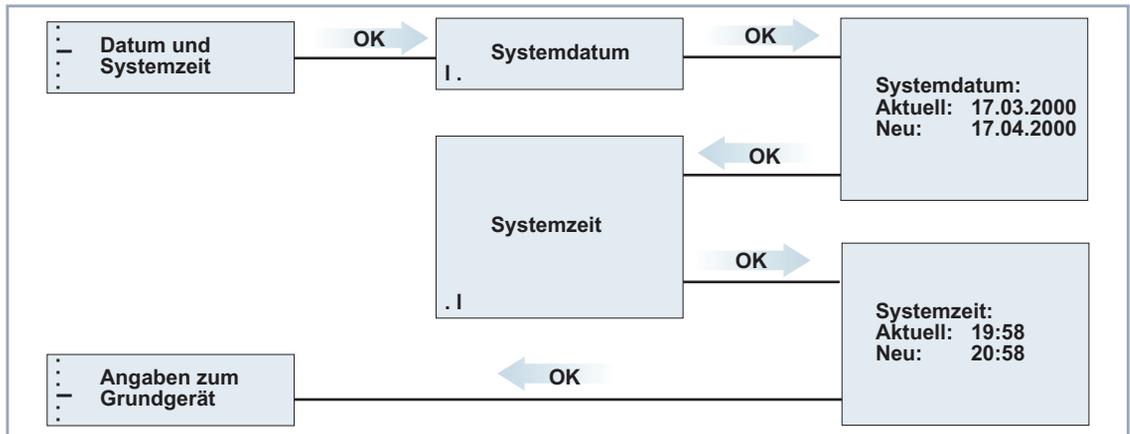


Bild 5-7: Menüs zum Eingeben von Datum/Systemzeit (mit Navigationsleisten)

■ Systemdatum

Hier stellen Sie das aktuelle Datum auf **X4000** 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 **X4000** 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:

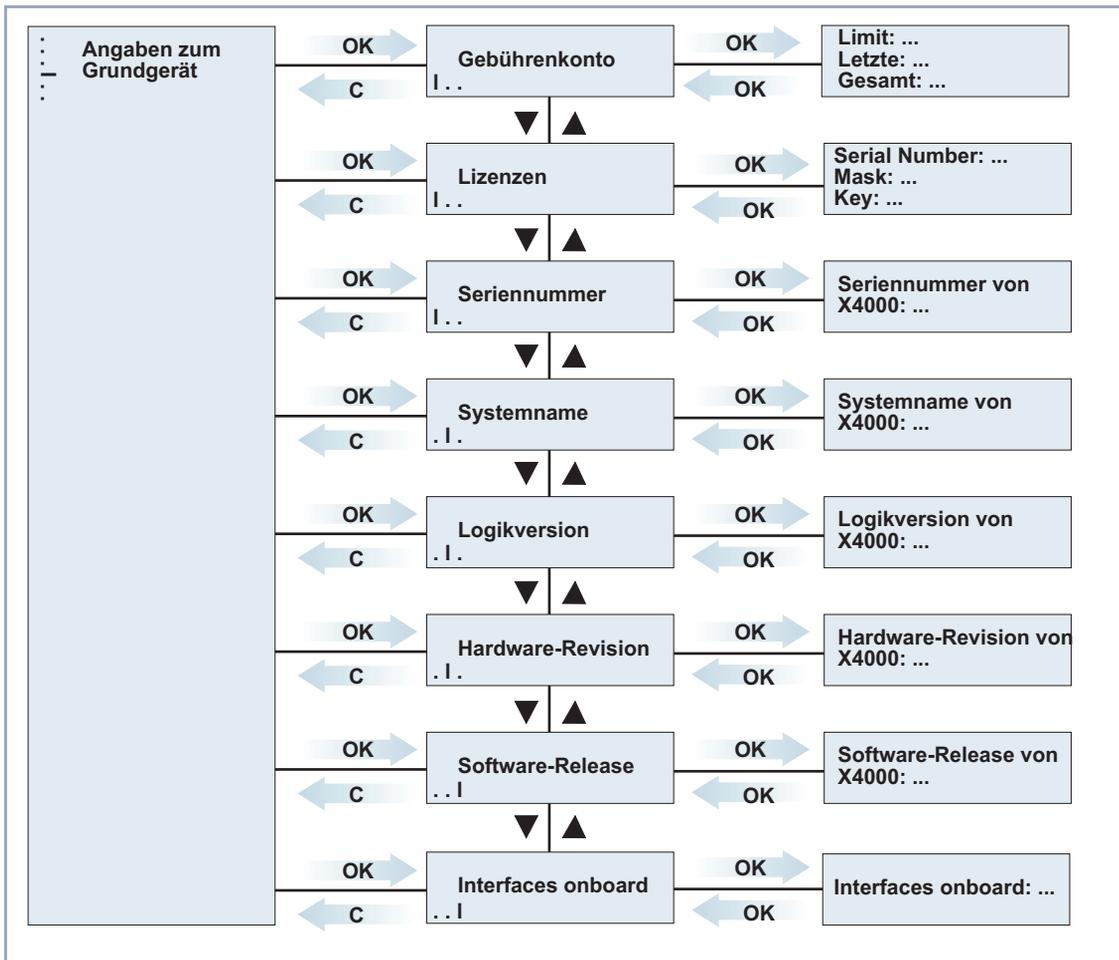


Bild 5-8: Menüs zum Monitoring des Grundgeräts (mit Navigationsleisten)

■ Gebührenkonto

Hier werden die Einstellungen für das Taschengeldkonto (Credits Based Accounting System, siehe [Kapitel 10.1.3, Seite 328](#)) angezeigt.

Limit: Eingestelltes Gebührenlimit.

Letzte: Kosten der letzten Verbindung.

Gesamt: Bisher angefallene Kosten.

■ Lizenzen

Hier werden die auf **X4000** eingetragenen Lizenzen angezeigt (siehe [Kapitel 7.1.1, Seite 121](#)).

■ Seriennummer

Hier wird die Seriennummer von **X4000** angezeigt.

■ Systemname

Hier wird der Systemname von **X4000** angezeigt (siehe [Kapitel 7.1.2, Seite 123](#)).

■ Logikversion

Hier wird die Version der Firmware-Logik von **X4000** angezeigt.

■ Hardware-Revision

Hier wird die Hardware-Revision von **X4000** angezeigt.

■ Software-Release

Hier wird die Version der System-Software von **X4000** angezeigt.

■ Interfaces onboard

Hier wird der Status der **X4000**-Hardware-Schnittstellen 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 **X4000**:



Bild 5-9: Menüs zum Monitoring von **X4000**

■ Aktuelle Temperatur

Hier wird die aktuelle Betriebstemperatur von **X4000** in °C 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 der MIB-Variable **sysX4ConfigTempAlarmTrap** für das Grundgerät (**Temp**) bzw. der MIB-Variablen **sysX4ConfigTempAlarmTrapMod1** und **sysX4ConfigTempAlarmTrapMod2** für die Erweiterungskarten (**Temp1** und **Temp2**) verändert werden. Bei Überschreiten dieser Temperatur erzeugt **X4000** Traps, die über das Netzwerk ausgewertet werden können.

5.4 Nützliche Short-Cuts

Durch Verwendung der Eingabetasten können Sie einige Aktionen durchführen:

5.4.1 Default-Screen festlegen

Standardmäßig wird nach Ablauf des Idletimers das Logo auf dem Display angezeigt. Um einen anderen Bildschirm des MMI als Default Screen zu verwenden, gehen Sie folgendermaßen vor:

- Zeigen Sie unter Verwendung der Eingabetasten den gewünschten Bildschirm an.
- Halten Sie die Taste **C** für die Dauer von drei Sekunden gedrückt.



Neuer
Default Screen
wurde ausgewählt

- Bestätigen Sie mit **OK**.
Der ausgewählte Bildschirm wird angezeigt und als Default Screen verwendet.

5.4.2 Konfiguration sichern

Gehen Sie folgendermaßen vor, um die aktuelle Konfiguration von **X4000** durch die Verwendung der Eingabetasten zu sichern.

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



Wollen Sie die neue
Konfiguration
sichern?

- Drücken Sie **OK**.

Die Konfiguration
wird gesichert ...

Konfiguration
gesichert

- Drücken Sie **OK**.

5.4.3 X4000 neustarten

Gehen Sie folgendermaßen vor, um **X4000** durch Verwendung der Eingabetasten neu zu starten:

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

ACHTUNG!
Wollen Sie X4000
wirklich rebooten?

- Drücken Sie **OK**.

System-Reboot in
5 Sekunden!

Nach 5 Sekunden wird der Neustart ausgeführt.

System-Reboot ...
Warten Sie, bis
X4000 wieder be-
triebsbereit ist!

6 Schnelle Konfiguration mit dem Configuration Wizard (Grundgerät)

Mit dem Configuration Wizard, der sich auf Ihrer BinTec Companion CD befindet, bietet Ihnen BinTec Communications AG eine komfortable Möglichkeit, **X4000** schnell und einfach in Betrieb zu nehmen. Sie können über die serielle Schnittstelle Ihres Windows-PC eine Grundkonfiguration erstellen, die alle wichtigen Einstellungen des Routers, den Zugang zum Internet über einen Internet Service Provider (ISP) sowie die Verbindung zu einem WAN-Partner (z. B. Firmenzentrale) beinhaltet. Tiefgehende Netzwerkkennnisse sind dabei nicht erforderlich, denn der Configuration Wizard führt Sie Schritt für Schritt durch die Konfiguration. Ein detailliertes Online-Hilfe-System, auf das Sie zu jedem Zeitpunkt der Konfiguration zugreifen können, und die graphische Unterstützung mit aussagekräftigen Darstellungen geben Ihnen zusätzlich Hilfestellung.

Der Configuration Wizard ist eine von mehreren Möglichkeiten, **X4000** zu konfigurieren. Der Zugang zu **X4000** erfolgt dabei über die serielle Schnittstelle. Beachten Sie bitte, daß Sie mit dem Configuration Wizard nur Ihre ISDN-BRI-Schnittstelle des Grundgeräts konfigurieren können! Für die Konfiguration von WAN-Verbindungen über die X.21/V.35/V.36-Schnittstelle bzw. die X.21bis-Schnittstelle, müssen Sie mit dem Setup Tool arbeiten. Die weiterführende Konfiguration ([Kapitel 8, Seite 193](#)) und die Einrichtung der Sicherheitsfunktionen ([Kapitel 10, Seite 319](#)) erfolgen im Anschluß mit dem Setup Tool.

In diesem Kapitel erfahren Sie, wie Sie:

- Ihre Konfiguration vorbereiten ([Kapitel 6.1, Seite 111](#))
- Windows-Software installieren und einrichten:
 - BRICKware for Windows installieren ([Kapitel 6.2, Seite 113](#))
 - **X4000** mit dem Configuration Wizard konfigurieren ([Kapitel 6.3, Seite 114](#))
- Eventuell zusätzliche Einstellungen an Ihren Rechnern vornehmen ([Kapitel 6.4, Seite 116](#))
 - Remote-CAPI-Schnittstelle konfigurieren ("[Remote-CAPI konfigurieren](#)", [Seite 116](#))

- RVS-COM Lite installieren ("[RVS-COM Lite installieren](#)", Seite 116)
- Rechner für WAN-Zugang einrichten ("[Mit X4000 ins Internet](#)", Seite 116)

Am Ende des Kapitels können Sie Ihre Konfiguration testen.

6.1 Konfiguration vorbereiten

Routereinstellungen Bevor Sie die eigentliche Konfiguration von **X4000** vornehmen, müssen Sie einige Daten über Ihren ISDN-Anschluß und Ihre Netzwerkumgebung kennen. Tragen Sie in den folgenden Tabellen Ihre eigenen Werte ein, um diese bei der Konfiguration schnell zu finden. Beispiele sind angegeben.

- ISDN-Rufnummern: Die Rufnummern Ihres ISDN-Anschlusses.
- IP-Adresse und Netzmaske von **X4000**: Falls Sie ein neues Netzwerk einrichten, können Sie einfach die Beispielwerte übernehmen.

Zugangsdaten	Beispielwert	Ihr Wert
ISDN-Rufnummern	<i>10, 11, 12</i>	
IP-Adresse von X4000	<i>192.168.1.254</i>	
Netzmaske von X4000	<i>255.255.255.0</i>	

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

Zugangsdaten	Beispielwert	Ihr Wert
Providername	<i>GoInternet</i>	
Einwahlnummer	<i>1234567</i>	
Anschlußkennung	<i>MyName</i>	
Paßwort	<i>TopSecret</i>	

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	<i>BigBoss</i>	
Einwahlnummer	<i>0911987654321</i>	
Lokaler Name	<i>LittleIndian</i>	

Zugangsdaten	Beispielwert	Ihr Wert
Paßwort	<i>Secret</i>	
Netzadresse(n) des Partners	<i>10.1.1.0</i>	
Netzmaske(n) des Partners	<i>255.255.255.0</i>	

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.

6.2 BRICKware installieren

BRICKware for Windows enthält den Configuration Wizard und weitere Windows-Hilfsprogramme.

- 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 für Windows sind, umfassen hauptsächlich Hilfsprogramme zur Konfiguration, Wartung und Diagnose von **X4000**. Für die Grundfunktion von **X4000** ist es nicht nötig, DIME Tools mit Windows automatisch starten zu lassen.

- Starten Sie den Configuration Wizard am Ende der Installation.



Eine detaillierte Beschreibung der Installation von BRICKware und die Beschreibung der einzelnen Komponenten finden Sie in [BRICKware for Windows](#) auf BinTec's WWW-Server unter Lösungen & Produkte, Sektion Download.

6.3 Grundlegende X4000-Konfiguration mit dem Configuration Wizard

Die Grundeinstellungen von **X4000** konfigurieren Sie schnell und einfach mit dem Configuration Wizard. Bitte beachten Sie: Wenn Sie eine Konfiguration bereits mit dem Wizard erstellt haben, kann der Wizard die voreingestellten Werte übernehmen. Am Ende überträgt er die Konfiguration zum Router und sichert sie zusätzlich auf dem PC.

Sie können die Konfiguration mit einem Quick-Modus oder mit einem Expert-Modus durchführen. Wenn Sie wenig Erfahrung mit Netzwerktechnologie haben, wählen Sie den Quick-Modus.

Wenn Sie BRICKware installiert haben und den Configuration Wizard aktivieren, erscheint folgendes Startfenster (wenn nicht, gehen Sie zu [Kapitel 6.2, Seite 113](#)):



Bild 6-1: Startfenster Configuration Wizard

Folgende Konfigurationenpunkte können Sie auswählen:

- Router-Grundkonfiguration
- Internetzugang

- Firmennetzanbindung (LAN-LAN Kopplung).

Die Router-Grundkonfiguration ist zwingend erforderlich. Sie bindet **X4000** in Ihr lokales Netzwerk ein und ermöglicht Kommunikationsanwendungen (CAPI).

- Wählen Sie die gewünschten Punkte aus und folgen Sie dann den Anweisungen am Bildschirm.



Achtung!

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

- Ändern Sie daher unbedingt Ihr Systempaßwort, wenn Sie dazu aufgefordert werden.
- Klicken Sie auf **Fertigstellen**. Damit haben Sie die grundlegende Konfiguration mit dem Configuration Wizard beendet.

Wenn Sie **X4000** bei der Konfiguration mit dem Configuration Wizard als DHCP-Server eingerichtet haben, muß den PCs am Ende der Konfiguration eine IP-Adresse zugewiesen werden. Unter Windows NT geschieht dies automatisch. Unter Windows 95/98 startet der Wizard das Programm WINIPCFG:

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

6.4 PC einrichten

Falls Sie während der Konfiguration Kommunikationsanwendungen (CAPI) ausgewählt haben, werden Sie jetzt aufgefordert, die CAPI-Konfiguration durchzuführen. CAPI ermöglicht Ihnen u. a. das Versenden und Empfangen von Faxen und eine Anrufbeantworterfunktion.

Remote-CAPI konfigurieren ➤ Starten Sie mit **Ja**. Tragen Sie im Register **Remote CAPI** die IP-Adresse von **X4000**, Benutzernamen und Paßwort der mit dem Configuration Wizard eingerichteten Nutzer der Kommunikationsanwendungen ein, falls die Werte nicht schon eingetragen sind. Klicken Sie auf **Use these values**. Klicken Sie auf **OK**.

RVS-COM Lite Um z. B. Faxdienste nutzen zu können, müssen Sie auch eine CAPI-Anwendung, z. B. RVS-Com Lite, installieren. RVS-Com Lite befindet sich auf Ihrer BinTec Companion CD.



Bitte beachten Sie: Es handelt sich dabei um eine Einzelplatzlizenz für RVS-COM Lite. Weitere Lizenzen können Sie über Ihren Händler beziehen.

COM-Port-Treiber Wenn Sie Ihr DFÜ-Netzwerk mit BinTec's Remote-CAPI nutzen wollen, stellt Ihnen RVS-Com Lite den dafür erforderlichen COM-Port-Treiber bereit.

RVS-COM Lite installieren ➤ Zur Installation von RVS-COM Lite klicken Sie im Setup-Programm auf **RVS-Com Lite** und befolgen Sie die Anweisungen. Eine Online-Hilfe ist vorhanden.

Mit X4000 ins Internet Sie können über **X4000** einen WAN-Zugang, z. B. ins Internet, für alle PCs herstellen, die sich mit **X4000** in einem Netzwerk befinden. Dazu müssen Sie auf allen PCs, die bei der Konfiguration nicht als DHCP-Clients eingerichtet wurden, **X4000** 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 **X4000** ein. Klicken Sie auf **Hinzufügen**. (Windows NT: Tragen Sie im Register **IP-Adresse** unter **Standardgateway** die IP-Adresse von **X4000** ein.)
- Tragen Sie im Register **DNS-Konfiguration** unter **Suchreihenfolge für DNS-Server** die IP-Adresse von **X4000** ein. Klicken Sie auf **Hinzufügen**, dann auf **OK**. Befolgen Sie die weiteren Anweisungen.

6.5 Konfiguration testen

Wenn Sie nun das serielle Kabel von **X4000** entfernen, haben Sie es geschafft! 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 **X4000** Verbindungen nur zu gewollten Zeiten aufbaut!

- Um unnötige Gebühren zu vermeiden, prüfen Sie, ob die im Configuration Wizard eingestellten Filter für Ihre Bedürfnisse ausreichend sind. Falls nicht, können Sie weitere Filter mit dem Setup Tool konfigurieren (Kapitel 10.2.8, Seite 349).
- Beobachten Sie die Leuchtanzeigen von **X4000** (vgl. Kapitel 3.4, Seite 63), benutzen Sie die Monitorfunktion des Setup Tools (vgl. Kapitel 10.1, Seite 320), fragen Sie Ihre Einstellungen am Display ab (vgl. Kapitel 5, Seite 93) oder prüfen Sie Ihre Einstellungen mit einem SNMP-Management-Tool.

LAN-Verbindung testen

- Testen Sie die Verbindung zu **X4000**. Klicken Sie im Startmenü Ihres PCs auf **Ausführen** und geben Sie `ping` gefolgt von einem Leerzeichen und der IP-Adresse von **X4000** ein, z. B. `ping 192.168.1.254`. Es erscheint ein Fenster mit dem Hinweis "**Reply from...**".

Internetzugang testen

- Testen Sie den Internetzugang, indem Sie im Browser www.bintec.de eingeben. Auf BinTec's Internetseiten finden Sie Neuigkeiten, Updates und weiterführende Dokumentation.

7 Grundkonfiguration des Grundgeräts mit dem Setup Tool

In diesem Kapitel erfahren Sie, wie Sie die grundlegenden Konfigurationsschritte für die Inbetriebnahme Ihres **X4000**-Grundgerätes mithilfe des Setup Tools durchführen.

Das Kapitel ist folgendermaßen aufgebaut:

- Grundlegende Routereinstellungen ([Kapitel 7.1, Seite 120](#))
Hier sind die Schritte beschrieben, die Sie für den Betrieb von **X4000** in jedem Fall durchführen müssen; unabhängig davon, in welcher Umgebung bzw. für welche Applikationen Sie **X4000** nutzen.
Die hier beschriebenen Schritte können Sie auch mit dem Configuration Wizard durchführen (siehe [Kapitel 6, Seite 109](#)).
- Wie geht's jetzt weiter? ([Kapitel 7.1.6, Seite 136](#))
Nachdem Sie die grundlegenden Routereinstellungen vorgenommen haben, können Sie sich mithilfe dieses Kapitels orientieren, wie Sie weitermachen können.
- WAN-Schnittstellen konfigurieren ([Kapitel 7.2, Seite 138](#))
Beschreibung, wie Sie die im **X4000**-Grundgerät integrierten WAN-Schnittstellen konfigurieren.
 - ISDN-BRI-Schnittstelle ([Kapitel 7.2.1, Seite 138](#)), einschließlich Verteilung der eingehenden Rufe auf Subsysteme und Benutzer ("[Incoming Call Answering](#)", [Seite 142](#))
 - Serielle Schnittstellen (X.21, V.35, V.36, X.21bis) ([Kapitel 7.2.2, Seite 151](#))
 - LAN-Schnittstelle zur Nutzung von ADSL ([Kapitel 7.2.3, Seite 157](#))
- WAN-Partner einrichten
 - Prinzipielle Vorgehensweise ([Kapitel 7.3, Seite 162](#))
 - Beispielkonfigurationen ([Kapitel 7.3.2, Seite 187](#))
- Konfiguration sichern ([Kapitel 7.4, Seite 191](#))

7.1 Grundlegende Routereinstellungen

Das Einrichten der grundlegenden Routereinstellungen betrifft nur **X4000** und Ihr lokales Netzwerk.

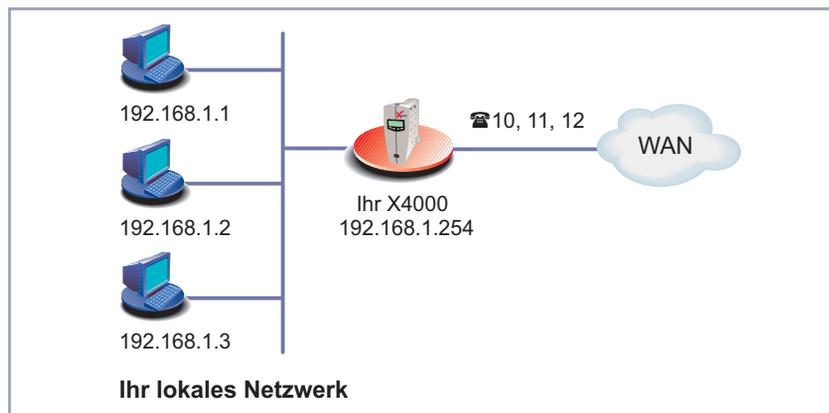


Bild 7-1: Grundlegende Routereinstellungen – **X4000** im LAN

Folgende Schritte sind erforderlich:

- Lizenz eintragen ([Kapitel 7.1.1, Seite 121](#))
- Systemdaten (z. B. Paßwörter) eintragen ([Kapitel 7.1.2, Seite 123](#))
- LAN-Schnittstelle konfigurieren ([Kapitel 7.1.3, Seite 126](#))
- **X4000** als DHCP-Server einrichten (optional) ([Kapitel 7.1.4, Seite 129](#))
- NetBIOS-Filter setzen (optional) ([Kapitel 7.1.5, Seite 132](#))

Was Sie an Vorbereitungen treffen sollten finden Sie in [Kapitel 6.1, Seite 111](#).

Was in Ihrem Netzwerk bzw. auf den PCs zu tun ist finden Sie in [Kapitel 6.4, Seite 116](#).

Los geht's:

7.1.1 Lizenz(en) eintragen

Lizenzkarte Nachdem Sie sich wie in [Kapitel 4.2, Seite 76](#) beschrieben auf **X4000** mit dem Benutzernamen `admin` eingeloggt und das Setup Tool mit `setup` aufgerufen haben, tragen Sie zunächst die Lizenzinformationen ein. Diese sind auf der mitgelieferten Lizenzkarte vermerkt. Damit schalten Sie die Funktionen von **X4000** frei.

➤ Gehen Sie zu **LICENSES**:

```

X4000 Setup Tool                                     BinTec Communications AG
[LICENSE]: Licenses                                 MyRouter

Available Licenses:
IP (builtin), STAC (valid), CAPI (valid), BRIDGE (valid)
IPX (valid)

Serialnumber      Mask      Key      State
101546            55       88PNUPZ  ok

ADD                DELETE    EXIT

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

```

Unter **Available Licenses** sind die auf **X4000** verfügbaren Subsysteme und deren Status (*builtin* - immer verfügbar, *valid* - freigeschaltet, *not_valid* - nicht freigeschaltet) aufgelistet.

Darunter sind die eingetragenen Lizenzen (**Serialnumber**, **Mask**, **Key**) abgebildet.

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

Subsysteme Folgende Subsysteme stehen prinzipiell auf **X4000** zur Verfügung:

Subsysteme	Bedeutung
IP	IP-Routing
OSPF	Open Shortest Path First (nur mit Zusatzlizenz)
TAF	Token Authentication Firewall (nur mit Zusatzlizenz)
TUNNEL	Virtual Private Networking VPN (nur mit Zusatzlizenz)
STAC	➤➤ STAC -➤➤ Datenkompression
CAPI	➤➤ Remote-CAPI -Schnittstelle, ermöglicht Kommunikationsanwendungen auf Ihrem Rechner, z. B. Faxe versenden und empfangen
BRIDGE	Bridging
X25	X.25 (nur mit Zusatzlizenz)
FRAME RELAY	Frame Relay (nur mit Zusatzlizenz)
IPX	➤➤ IPX -Routing

Tabelle 7-1: Subsysteme

ToDo Gehen Sie folgendermaßen vor, um eine Lizenz einzutragen:

- Fügen Sie einen neuen Eintrag mit **ADD** hinzu.
Ein weiteres Menüfenster erscheint.
- Wie auf Ihrer Lizenzkarte vermerkt, geben Sie **Serial Number**, **Mask** und **Key** 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, haben Sie sich wahrscheinlich vertippt.

➤ Versuchen Sie es erneut.

7.1.2 Systemdaten eintragen

Systemname,... Tragen Sie als nächstes die grundlegenden Systemdaten von **X4000** ein.

➤ Gehen Sie zu **SYSTEM:**

X4000 Setup Tool	BinTec Communications AG
[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 Teile des Menüs sind für diesen Konfigurationsschritt interessant:

Feld	Bedeutung
System Name	Definiert den Systemnamen von X4000 , wird auch als PPP-Host-Name benutzt. Erscheint beim Einloggen auf X4000 als Eingabe-Prompt. Wenn kein Systemname gesetzt ist, erscheint beim Einloggen mit dem Benutzernamen <code>admin</code> ein Warnhinweis.
Local PPP ID	Diese Eintragung ist zur Identifizierung von X4000 nötig, wenn eine nicht-partnerspezifische PPP-Authentisierung (z. B. PAP oder CHAP) durchgeführt wird (siehe Kapitel 8.1.3, Seite 200).
Location	(optional) Gibt an, wo sich X4000 befindet.
Contact	(optional) Gibt die zuständige Kontaktperson an. Wenn die Person von der HTTP-Statusseite von X4000 aus erreichbar sein soll (siehe Kapitel 10.1.4, Seite 332), muß hier eine gültige E-Mail-Adresse eingetragen werden.

Tabelle 7-2: **SYSTEM**

Paßwörter Im Untermenü **SYSTEM** ➔ **PASSWORD SETTINGS** geben Sie die Paßwörter für **X4000** ein:

Feld	Bedeutung
admin Login Password	Paßwort für Benutzername <code>admin</code> .
read Login Password	Paßwort für Benutzername <code>read</code> .
write Login Password	Paßwort für Benutzername <code>write</code> .
HTTP Server Password	Paßwort für die HTTP-Statusseite von X4000 .

Tabelle 7-3: **SYSTEM** ➔ **PASSWORD SETTINGS**

**Achtung!**

Alle BinTec-Router werden mit gleichem Benutzernamen und Paßwort ausgeliefert. Sie sind daher nicht gegen einen unauthorisierten Zugriff geschützt, solange die Paßwörter nicht geändert wurden. Die Vorgehensweise bei der Änderung von Paßwörtern ist unter "[Paßwortänderung](#)", [Seite 85](#) beschrieben.

- Ändern sie unbedingt die Paßwörter, um unberechtigten Zugriff auf **X4000** zu verhindern.

Die Befugnisse der möglichen Benutzernamen und Paßwörter finden Sie in [Kapitel 4.2, Seite 76](#).

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

- Geben Sie **System Name** von **X4000** 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.
- Geben Sie **HTTP Server Password** ein.
- Bestätigen Sie mit **SAVE**.
- Bestätigen Sie mit **SAVE**.

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

Weiterführende Konfiguration

Im Menü **SYSTEM** ➤ **EXTERNAL ACTIVITY MONITOR** finden Sie die Einstellungen, die nötig sind, um **X4000** mit dem Windows-Tool Activity Monitor überwachen zu können (siehe [Kapitel 10.1.6, Seite 334](#) bzw. [BRICKware for Windows](#)).

Im Menü **SYSTEM** ► **EXTERNAL SYSTEM LOGGING** finden Sie Einstellungen für Syslog-Messages (siehe [Kapitel 10.1.1, Seite 320](#)).

Im Menü **SYSTEM** ► **KEEPALIVE MONITORING** finden Sie Einstellungen für die Funktion Keepalive Monitoring (siehe [Kapitel 8.2.11, Seite 243](#)).

Im Menü **SYSTEM** ► **TIME AND DATE** finden Sie Einstellungen zur manuellen Eingabe von Uhrzeit und Datum auf **X4000** (siehe [Kapitel 8.3.1, Seite 249](#)).

7.1.3 LAN-Schnittstelle konfigurieren

- IP-Adresse,
- Netzmaske,
- Encapsulation

Konfigurieren Sie als nächstes die LAN-Schnittstelle (10/100 Base-T Ethernet) von **X4000**. Die LAN-Schnittstelle ist die physikalische Schnittstelle zum lokalen Netzwerk. Im folgenden Menü geben Sie Ihrem Router die Adresse, unter der er im LAN zu erreichen ist. Solange Ihr Router diese Eintragungen nicht hat, kann er von anderen Hosts im Netzwerk nicht erkannt werden.

Falls Ihr **X4000** an ein LAN angeschlossen ist, das aus zwei Teilnetzen besteht, sollten Sie ihm für das zweite Teilnetz eine **Second Local IP Number** und eine **Second Local Netmask** eintragen. Zur Erläuterung des Sachverhalts beachten Sie bitte das folgende Beispiel:

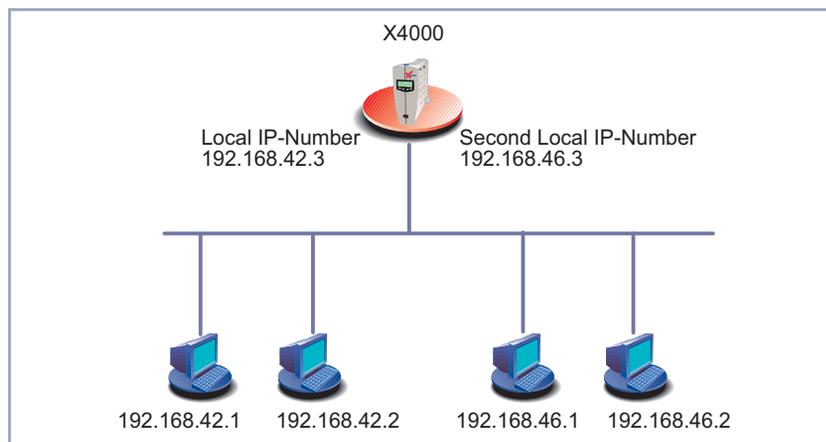


Bild 7-2: **X4000** mit zwei verschiedenen lokalen IP-Adressen

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 **X4000** 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 **X4000** schon vor der Grundkonfiguration IP-Adresse und Netzmaske über das MMI eingetragen. Überprüfen Sie trotzdem die Eintragungen im folgenden Menü.

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

X4000 Setup Tool	BinTec Communications AG
[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
IPX-Configuration	
local IPX-Netnumber	0
Encapsulation	none
Bridging	disabled
Advanced Settings>	
SAVE	CANCEL
Enter IP address (a.b.c.d or resolvable hostname)	

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

Folgende Teile des Menüs sind für diesen Konfigurationsschritt interessant:

Feld	Bedeutung
local IP-Number	IP-Adresse von X4000 im LAN.
local Netmask	Netzmaske des Netzwerkes, in dem sich X4000 mit local IP-Number befindet.
Second Local IP-Number	Zweite IP-Adresse von X4000 im LAN.
Second Local Netmask	Netzmaske des Netzwerkes, in dem sich X4000 mit Second Local IP-Number befindet.
Encapsulation	<p>Definiert, welche Art von Header den IP-Paketen, die über diese LAN-Schnittstelle laufen, hinzugefügt wird. Mögliche Werte:</p> <ul style="list-style-type: none"> ■ <i>Ethernet II</i> (entspricht IEEE 802.3) ■ <i>Ethernet SNAP</i> <p>I. A. können Sie den Standard-Wert <i>Ethernet II</i> belassen. Mit <i>Ethernet II</i> heißt die LAN-Schnittstelle en1, mit <i>Ethernet SNAP</i> en1-snap.</p>
Mode	<p>Definiert den Modus, in dem die LAN-Schnittstelle betrieben wird. Mögliche Werte:</p> <ul style="list-style-type: none"> ■ <i>Auto</i> (Standardwert): Automatische Erkennung der LAN-Parameter ist aktiviert, die LAN-Schnittstelle wird im passenden Modus betrieben. ■ <i>10 MBit Half Duplex</i> ■ <i>10 MBit Full Duplex</i> ■ <i>100 MBit Half Duplex</i> ■ <i>100 MBit Full Duplex</i> <p>In der Regel sollten Sie den voreingestellten Wert <i>Auto</i> belassen.</p>

Tabelle 7-4: **CM-100BT, FAST ETHERNET**

ToDo Gehen Sie folgendermaßen vor, um die LAN-Schnittstelle von **X4000** zu konfigurieren:

- Geben Sie **local IP-Number** von **X4000** 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 gespeichert.

Weiterführende Konfiguration Wenn Sie das ➤➤ **Protokoll** IPX verwenden, finden Sie Erläuterungen zur Konfiguration der LAN-Schnittstelle für IPX in [Kapitel 8.4, Seite 278](#).

Informationen zu Bridging finden Sie in der [Software Reference](#).

Im Menü **CM-100BT, FAST ETHERNET** ➤ **ADVANCED SETTINGS** finden Sie Einstellungen zu Routing Information Protocol RIP (siehe [Kapitel 8.2.8, Seite 236](#)), IP-Accounting, Proxy ARP (siehe [Kapitel 8.2.10, Seite 241](#)) und Backroute Verification (siehe [Kapitel 10.2.10, Seite 367](#)).

Wie Sie die LAN-Schnittstelle für ADSL-Verbindungen über den T-DSL-Anschluß der Deutschen Telekom nutzen, finden Sie in [Kapitel 7.2.3, Seite 157](#).

7.1.4 X4000 als DHCP-Server einrichten

IP-Adressen im LAN Jeder Rechner in Ihrem ➤➤ **LAN** benötigt, wie auch **X4000**, eine eigene IP-Adresse. Wenn Sie **X4000** als ➤➤ **DHCP** (Dynamic Host Configuration Protocol)-Server einrichten, vergibt **X4000** 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 **X4000** zugewiesen. Sie müssen den Rechnern keine festen IP-Adressen zuweisen, der Konfigurationsaufwand für Ihr Netzwerk verringert sich. Dazu richten Sie einen Pool an IP-Adressen ein, aus dem **X4000** 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.

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

X4000 Setup Tool	BinTec Communications AG
[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, der der folgende Adreß-Pool zugewiesen wird. Wenn ein Adreß-Request über Interface eingeht, wird eine der Adressen aus dem Adreß-Pool zugeteilt.
IP Address	Erste IP-Adresse des Adreß-Pools.
Number of consecutive addresses	Anzahl der IP-Adressen im Adreß-Pool, einschließlich der ersten IP-Adresse (IP Address).
Lease Time (Minutes)	Legt fest, wie lange eine Adresse aus dem Pool einem Host zugewiesen wird. Nachdem Lease Time (Minutes) abgelaufen ist, kann die Adresse anderweitig vergeben werden.
MAC Address	(optional) Nur bei Number of consecutive addresses = 1 : Nur dem Gerät mit MAC Address wird IP Address zugewiesen.
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 X4000 mitgegeben.
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 <i>not specified</i> übernehmen. Eine detaillierte Beschreibung dieser Funktion finden Sie in der Software Reference .

Tabelle 7-5: **IP** ➤ **IP ADDRESS POOL LAN (DHCP)** ➤ **ADD**

ToDo Machen Sie folgende Eintragungen, wenn Sie **X4000** als DHCP-Server einrichten wollen:

- 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)**, wo die IP-Adreß-Pools aufgelistet sind. Die Eintragungen sind gespeichert, Sie haben einen Adreßpool mit 8 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.

7.1.5 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**) aufgebaut werden, um WINS-Requests von Rechnern in Ihrem Netzwerk weiterzugeben. D. h. **X4000** fragt beim ISP nach, welcher ➤➤ **Hostname** einer IP-Adresse zugeordnet werden kann. Da der ISP WINS-Namen nicht auflösen kann, sind diese Verbindungen unnötig, kosten aber Gebühren.

Ausführliche Erläuterungen zum Thema ➤➤ **Filter** und Sicherheit finden Sie in [Kapitel 10.2.8, Seite 349](#).

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



Achten Sie darauf, daß Sie sich beim Konfigurieren der Filter nicht selbst ausperren:

- Greifen Sie zur Filter-Konfiguration über die serielle Schnittstelle oder ISDN-Login auf **X4000** zu.
- Wenn Sie trotzdem über Ihr LAN (z. B. telnet) auf **X4000** 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**:

X4000 Setup Tool		BinTec Communications AG	
[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			

ToDo Machen Sie folgende Eintragungen, 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.

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

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

X4000 Setup Tool		BinTec Communications AG	
[IP][ACCESS][RULE][ADD]: Configure IP Access Rules		MyRouter	
Action	deny M		
Filter	wrong_dns (1)		
	SAVE	CANCEL	
Use <Space> to select			

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

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

- Bestätigen Sie mit **SAVE**.

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

Definieren Sie nun eine zweite Regel wie folgt:

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

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

```

X4000 Setup Tool                               BinTec Communications AG
[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
    
```

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

```

X4000 Setup Tool                               BinTec Communications AG
[IP][ACCESS][INTERFACES]: Configure First Rule  MyRouter

Configure first rules for interfaces

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

EXIT

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

ToDo Machen Sie folgende Eintragungen:

- Wählen Sie die LAN-Schnittstelle von **X4000** (*en1* bzw. *en1-snap*) und bestätigen Sie mit der **Eingabetaste**.
- Wählen Sie **First Rule** aus: *RI 1 FI 1 (wrong_dns)*.
- Bestätigen Sie mit **SAVE**.

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

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

Sie befinden sich wieder im Hauptmenü.

Die Konfiguration der grundlegenden Routereinstellungen ist abgeschlossen.

7.1.6 Wie geht's jetzt weiter?

Nachdem Sie **X4000** für Ihr LAN konfiguriert haben, können Sie die folgenden Schritte durchführen, um WAN-Verbindungen zu ermöglichen.

- Konfigurieren Sie die WAN-Schnittstelle(n) von **X4000**, die Sie nutzen möchten:
 - ISDN-BRI-Schnittstelle ([Kapitel 7.2.1, Seite 138](#))
 - X.21/V.35/V.36-Schnittstelle bzw. X.21bis-Schnittstelle (seriell) ([Kapitel 7.2.2, Seite 151](#))
 - LAN-Schnittstelle für ADSL-Verbindungen ([Kapitel 7.2.3, Seite 157](#) bzw. [Kapitel 9.3.2, Seite 299](#))
- WAN-Partner konfigurieren ([Kapitel 7.3, Seite 162](#)).
Konfigurationsbeispiele:
 - ISP T-Online ("[Internetzugang über T-Online](#)", [Seite 187](#))
 - ISP CompuServe ("[Internetzugang über CompuServe](#)", [Seite 189](#))

- Konfigurieren Sie gegebenenfalls die Schnittstellen Ihrer Erweiterungskarte ([Kapitel 9, Seite 287](#))
- Möglichkeiten für weiterführende Konfiguration finden Sie in [Kapitel 8, Seite 193](#).
- Die Konfiguration von Sicherheitsfunktionen und Firewall finden Sie in [Kapitel 10, Seite 319](#).
- Wenn Sie mit dem **X4000**-Grundgerät Kommunikationsanwendungen auf den Hosts im LAN ermöglichen wollen (z. B. RVS COM Lite), müssen Sie auf den Hosts die Remote-CAPI-Konfiguration durchführen (siehe [Kapitel 6.4, Seite 116](#)) und die Zuordnung der Rufnummern entsprechend durchführen ("Incoming Call Answering", [Seite 142](#)).
- Nach Beenden der Konfiguration sollten Sie auf jeden Fall Ihre Konfigurationsdatei sichern ([Kapitel 7.4, Seite 191](#))

7.2 WAN-Schnittstellen konfigurieren

Im folgenden finden Sie die Konfigurationsschritte, die zum Einrichten der WAN-Schnittstellen von **X4000** erforderlich sind, Schritt für Schritt beschrieben.

Das Grundgerät verfügt über folgende WAN-Schnittstellen:

- ISDN-BRI-Schnittstelle (siehe [Kapitel 7.2.1, Seite 138](#))
- Zwei Serielle Schnittstellen: X.21/V.35/V.36-Schnittstelle und X.21bis-Schnittstelle (siehe [Kapitel 7.2.2, Seite 151](#))
- ADSL** ■ Zusätzlich können Sie die LAN-Schnittstelle als Schnittstelle zum WAN konfigurieren, indem Sie mit PPP-over-Ethernet eine Anbindung an T-DSL, dem ADSL-Anschluß der Deutschen Telekom, ermöglichen (siehe [Kapitel 7.2.3, Seite 157](#)).
Falls Sie eine LAN-Erweiterungskarte einsetzen, beachten Sie bitte [Kapitel 9.3.2, Seite 299](#).

Durch Einbau einer Erweiterungskarte können gegebenenfalls weitere WAN-Schnittstellen auf **X4000** genutzt werden, beachten Sie bitte [Kapitel 9, Seite 287](#).

7.2.1 ISDN-BRI-Schnittstelle konfigurieren

Die ISDN-BRI-Schnittstelle von **X4000** 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 **X4000** mit, wie auf eingehende Rufe aus dem WAN reagiert werden soll.

Autokonfiguration, ISDN Switch Type, ... Machen Sie zunächst die Einstellungen für Ihren ISDN-Anschluß:
➤ Gehen Sie zu **CM-1BRI, ISDN S0**.

```
X4000 Setup Tool                               BinTec Communications AG
[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 hat folgende Felder:

Feld	Bedeutung
Result of Autoconfiguration	Status der ISDN-Autokonfiguration. Die automatische ►► D-Kanal -Erkennung läuft, bis eine Einstellung gefunden wird bzw. bis das ISDN-Protokoll unter ISDN switch type manuell eingegeben ist.
ISDN Switch Type	<p>Definiert das ISDN-►► Protokoll, das Ihnen Ihre Telefongesellschaft zur Verfügung stellt. Folgende Einstellungen sind möglich:</p> <ul style="list-style-type: none"> ■ <i>autodetect on bootup</i>: automatische D-Kanalerkennung (Standardeinstellung) ■ <i>Euro ISDN point to multipoint</i>: Euro-ISDN an einem Mehrgeräteanschluß ■ <i>Euro ISDN point to point</i>: Euro-ISDN an einem Anlagenanschluß ■ <i>none</i> ■ <i>leased line B1 channel (64S)</i>: Festverbindung über B-Kanal 1 ■ <i>leased line B1+B2 channel (64S2)</i>: Festverbindung über beide B-Kanäle ■ <i>leased line D+B1+B2 channel (TS02)</i>: Festverbindung über D-Kanal und beide B-Kanäle ■ <i>leased line B1+B2 different endpoints (Digital 64S mit Doppelanschaltung)</i>: 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: <ul style="list-style-type: none"> ■ <i>leased dte</i> (Standardwert) ■ <i>leased dce</i>
B-Channel 1	Einstellung des ersten ►► B-Kanals . Mögliche Werte: <ul style="list-style-type: none"> ■ <i>dialup</i> (Standardwert) ■ <i>not used</i> ■ <i>leased dte</i> ■ <i>leased dce</i>
B-Channel 2	Einstellung des zweiten B-Kanals. Mögliche Werte: <ul style="list-style-type: none"> ■ <i>dialup</i> (Standardwert) ■ <i>not used</i> ■ <i>leased dte</i> ■ <i>leased dce</i>

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

ToDo Machen Sie folgende Eintragungen:

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

Mit dieser Einstellung nutzt **X4000** die automatische D-Kanal-Erkennung. Unter **Result of Autoconfiguration** erscheint *running*, solange die D-Kanal-Erkennung läuft. Danach wird die gefundene Einstellung angezeigt, z. B. *Euro ISDN, point to multipoint*.



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

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

- Wählen Sie gegebenenfalls **D-Channel** aus.
- Wählen Sie **B-Channel 1** aus: z. B. *dialup*.
- Wählen Sie **B-Channel 2** aus: z. B. *dialup*.



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** ausgewählt haben und die Werte änderbar sind.

- Bestätigen Sie mit **SAVE**.
Sie befinden sich wieder im Hauptmenü. Die Eintragungen sind gespeichert.

Incoming Call Answering

Falls Sie die ISDN-BRI-Schnittstelle für Wählverbindungen verwenden, müssen Sie als nächstes **X4000** mitteilen, wie auf eingehende Rufe aus dem ISDN reagiert werden soll. Entsprechend den Einstellungen in den folgenden Menüs verteilt **X4000** die eingehenden Rufe auf die internen Dienste.

X4000 unterstützt die Dienste:

- PPP (Routing):
Der Dienst ➤➤ **PPP** ist der allgemeine Routing-Dienst von **X4000**. 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 Netzwerkes aufzubauen.



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

■ ISDN-Login:

Der Dienst >> **ISDN-Login** ermöglicht eingehenden Daten-Rufen Zugang zur >> **SNMP-Shell** von **X4000**. So kann **X4000** aus der Ferne konfiguriert und gewartet werden.

■ CAPI:

Der Dienst >> **CAPI** ermöglicht eingehenden und ausgehenden Daten- und Sprach-Rufen eine Verbindung mit Kommunikationsanwendungen auf Hosts im LAN, die auf die >> **Remote-CAPI-Schnittstelle** von **X4000** zugreifen. So können beispielsweise mit **X4000** verbundene Hosts Faxe empfangen und senden.

Um mit dem **X4000**-Grundgerät CAPI-Applikationen (z. B. RVS COM Lite) 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 6.4, Seite 116](#)).

Wenn ein Ruf eingeht, überprüft **X4000** zunächst die Called Party Number (CPN) und die Art des Anrufs (Daten- oder Sprach-Ruf). CPN ist die Rufnummer, die der Partner gewählt hat, um **X4000** zu erreichen. Anschließend wird

der Ruf an den passenden Dienst weitergeleitet (siehe auch [Bild 7-3](#), [Seite 144](#)).

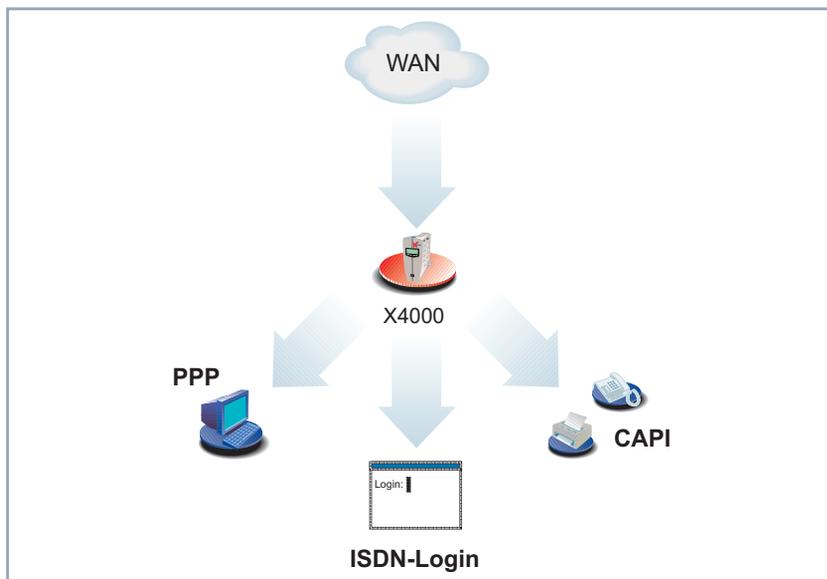


Bild 7-3: Verteilung der eingehenden Rufe

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 7-7: 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" und 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 Users Concept nutzen (siehe [Kapitel 8.1.2, Seite 196](#)). Den Benutzer "default" ohne Paßwort sollten Sie dann löschen.



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

Machen Sie nun die Eintragungen für Incoming Call Answering:

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

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

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

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

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

Ein weiteres Menüfenster erscheint:

X4000 Setup Tool	BinTec Communications AG	
[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 7-9, Seite 149 .
Number	Rufnummer, unter der der oben eingetragene Dienst (Item) erreicht werden kann.
Mode	Modus, mit dem X4000 den Ziffernvergleich von Number mit der Called Party Number des eingehenden Rufes durchführt: <ul style="list-style-type: none"> ■ <i>right to left</i> (Standardwert) ■ <i>left to right (DDI)</i>: Immer auswählen, wenn X4000 mit einem Point-to-Point-Anschluß (Anlagenanschluß) verbunden ist.
Username	(nur bei Item = <i>CAPI 1.1 EAZ 0...9 Mapping</i>) CAPI-Benutzername. Nur erforderlich, wenn Sie das CAPI User Concept nutzen wollen (siehe Kapitel 7.1.2, Seite 192).
Bearer	Art des eingehenden Rufes. Mögliche Werte: <ul style="list-style-type: none"> ■ <i>data</i>: Daten-Ruf ■ <i>voice</i>: Sprach-Ruf ■ <i>any</i>: sowohl Daten- als auch Sprach-Ruf

Tabelle 7-8: **CM-1BRI, ISDN S0** ➤ **INCOMING CALL ANSWERING** ➤ **ADD**

Das Feld **Item** enthält folgende Auswahlmöglichkeiten:

Mögliche Werte	Bedeutung
<i>PPP (routing)</i>	Standardeinstellung für ►► PPP -Routing. Zutreffend auch für die unten genannten PPP-Verbindungen.
<i>ISDN Login</i>	Ermöglicht Einloggen mit ►► isdnlogin .
<i>PPP 64k</i>	Ermöglicht 64 kbps PPP-Datenverbindungen.
<i>PPP 56k</i>	Ermöglicht 56 kbps PPP-Datenverbindungen.
<i>PPP Modem</i>	(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 Modem Profile 1, die im Menü MODEM ► PROFILE CONFIGURATION ► PROFILE 1 getroffen wurden.
<i>PPP DOVB</i>	Data transmission Over Voice Bearer – nützlich z. B. in den USA, wo Sprachverbindungen manchmal billiger sind als Datenverbindungen.
<i>PPP V.110 (1200...38400)</i>	Ermöglicht PPP-Verbindungen mit V.110 mit Bit-Raten von 1200 bps, 2400 bps,..., 38400 bps.
<i>Pots</i>	Auf X4000 nicht verfügbar.
<i>PPP Modem Profile 1...8</i>	(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 Modem Profile 1... 8, die im Menü MODEM ► PROFILE CONFIGURATION ► PROFILE 1...8 getroffen wurden.

Mögliche Werte	Bedeutung
<i>CAPI 1.1 EAZ 0...9 Mapping</i>	Ermöglicht Verbindungen mit Remote-CAPI-Applikationen. Nur erforderlich für CAPI 1.1-Applikationen.
<i>X.25 PAD</i>	Ermöglicht Datenverbindungen mit X.25 PAD.

Tabelle 7-9: **Item**

Achten Sie darauf, unter **Number** die richtige Nummer, d. h. die Nummer, die auch wirklich bei **X4000** ankommt, einzutragen! Wenn **X4000** z. B. an einer **TK-Anlage** angeschlossen ist, kommt nur die Nebenstellenummer bei **X4000** an.

Wenn Sie sich nicht sicher sind, welche Nummer bei **X4000** wirklich ankommt, gehen Sie folgendermaßen vor:

- Rufen Sie mit einem herkömmlichen Telefon **X4000** 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 **X4000** 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 **X4000** 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, d.h. es genügt ein einziger Eintrag.

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

ToDo Machen Sie folgende Eintragungen:

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

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

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

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

Damit haben Sie Incoming Call Answering konfiguriert, **X4000** verteilt die eingehenden Rufe an die internen Dienste.

Weiterführende Konfiguration Unter **CM-1BRI, ISDN S0** ► **ADVANCED SETTINGS** finden Sie Einstellungen für X.31-TEI (siehe [Kapitel 8.1.4, Seite 203](#)).

Falls Sie eine Festverbindung nutzen, können Sie mit dem Feature Bandwidth on Demand u. a. eine Backuplösung realisieren (siehe [Kapitel 8.2.3, Seite 207](#)). Wenn Sie diese Möglichkeit nutzen, wird bei Ausfall der Festverbindung eine Wählverbindung zum Verbindungspartner aufgebaut.

7.2.2 Serielle Schnittstellen konfigurieren

Das **X4000**-Grundgerät verfügt über zwei serielle WAN-Schnittstellen:

■ Der erste serielle Port (Setup-Tool-Menü **CM-SERIAL, SERIAL** ► **UNIT 0**) ist als Schnittstelle der Typen

- X.21/V.11
- V.35/V.11
- V.36/V.11

verwendbar.

Durch die Einstellung im Setup-Tool-Feld **Connector** (siehe [Tabelle 7-11, Seite 155](#)) kann der Port so umgestellt werden, daß **X4000** 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.

■ Der zweite serielle Port (Setup-Tool-Menü **CM-SERIAL, SERIAL** ► **UNIT 1**) ist als Schnittstelle des Typs

- X.21bis/V.28

verwendbar.

Bei diesem Port kann die Umstellung vom DCE- in den DTE-Modus und umgekehrt nur über die Verwendung eines DCE- bzw. DTE-Kabels verwirklicht werden.

	Interface Type	DTE-Modus	DCE-Modus
Port 1	X.21 V.35 V.36	Standardkabel Connector = dte	Standardkabel Connector = dce
Port 2	X.21bis	DTE-Kabel	DCE-Kabel

Tabelle 7-10: Funktionalität der seriellen Ports

Konfiguration mit dem Setup Tool

Um die X.21/V.35/V.36- bzw. X.21bis-Schnittstelle von **X4000** zu konfigurieren, steht folgendes Menü zur Verfügung:

X4000 Setup Tool	BinTec Communications AG
[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	<p>Definiert den Schnittstellentyp des verwendeten Ports. Mögliche Werte:</p> <ul style="list-style-type: none"> ■ <i>none</i> (Standardwert): Schnittstelle wird nicht genutzt. ■ <i>X.21</i>: Nutzung als X.21/V.11-Schnittstelle ■ <i>V.35</i>: Nutzung als V.35/V.11-Schnittstelle ■ <i>V.36</i>: Nutzung als V.36/V.11-Schnittstelle ■ <i>X.21bis</i>: Nutzung als X.21bis/V.28-Schnittstelle
Connector	<p>Legt die Pin-Belegung des Ports fest (siehe Kapitel 13.2.4, Seite 409).</p> <p>Nur beim ersten seriellen Port CM-SERIAL, SERIAL ▶ UNIT 0 kann durch diese Einstellung die Pin-Belegung beeinflusst werden, beim zweiten seriellen Port CM-SERIAL, SERIAL ▶ UNIT 1 muß ein entsprechendes DCE- bzw. DTE-Kabel verwendet werden!</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ■ <i>dte</i> (Standardwert): Die Pins sind als DTE-Schnittstelle belegt. Diese Einstellung ist z. B. dann erforderlich, wenn X4000 mit einem öffentlichen Datennetz verbunden ist (z. B. Datex-P in Deutschland). ■ <i>dce</i>: Die Pins sind als DCE-Schnittstelle belegt. Dies ist erforderlich, um ein DTE-konfiguriertes Gerät bedienen zu können.

Feld	Bedeutung
Clock Mode	<p>Definiert, welcher Verbindungspartner das Taktsignal zur Synchronisation zwischen Sender und Empfänger gibt. Mögliche Werte:</p> <ul style="list-style-type: none"> ■ <i>auto</i> (Standardwert): Die Einstellung richtet sich nach der für Connector getroffenen Auswahl: <ul style="list-style-type: none"> – X4000 gibt das Taktsignal, wenn Connector = <i>dce</i>. – X4000 empfängt das Taktsignal, wenn Connector = <i>dte</i>. <p>In der Regel können Sie diese Einstellung übernehmen.</p> ■ <i>extern</i>: X4000 empfängt das Taktsignal, unabhängig von der unter Connector gewählten Einstellung. ■ <i>intern</i>: X4000 gibt das Taktsignal, unabhängig von der unter Connector gewählten Einstellung.
Speed	<p>Übertragungsrate der Verbindung, skalierbar von <i>2400 bit/s</i> bis <i>8 Mbit/s</i>.</p> <p>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.</p> <p>Standardwert: <i>64000 bit/s</i></p>

Feld	Bedeutung
Layer 2 Mode	<p>Definiert den Wert des HDLC-Adressfelds in gesendeten Kommando-Frames (Schicht 2). Mögliche Werte:</p> <ul style="list-style-type: none"> ■ <i>auto</i> (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). ■ <i>dte</i>: Das Adressfeld hat den Wert für DTE. ■ <i>dce</i>: Das Adressfeld hat den Wert für DCE.
Interface Leads	<p>Legt fest, ob X4000 den Status der Schnittstellenleitung überprüft. Bei beiden Verbindungspartnern sollte der gleiche Wert eingestellt sein. Mögliche Werte:</p> <ul style="list-style-type: none"> ■ <i>enabled</i>: Der Status der Signalleitung (I bei X.21, CTS bei V.35, V.36 und X.21bis) wird überprüft und als L1State übernommen. ■ <i>disabled</i> (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 7-11: **CM-SERIAL, SERIAL** ➤ **UNIT 0** bzw. **CM-SERIAL, SERIAL** ➤ **UNIT 1**

	Connector = DTE (Standardwert)	Connector = DCE	Port
Funktion	DTE	DCE	1
Kabel	Standardkabel		
Pinbelegung	X.21: siehe "DB-15-Stecker für X.21", Seite 411 V.35: siehe "M34-Stecker für V.35", Seite 412 V.36: siehe "DB-37-Stecker für V.36", Seite 413		
Funktion	DTE	DCE	2
Kabel	DTE-Kabel	DCE-Kabel	
Pinbelegung	X.21bis: siehe "DB-25-Stecker für X.21bis", Seite 415		

Tabelle 7-12: Verwendung von **Connector** im Setup Tool

ToDo Gehen Sie folgendermaßen vor, um die seriellen Schnittstellen zu konfigurieren (die angegebenen Beispielswerte sind erforderlich, wenn Sie **X4000** 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 Backuplösung realisieren (siehe [Kapitel 8.2.3](#),

[Seite 207](#)). Wenn Sie diese Möglichkeit nutzen, wird bei Ausfall der Festverbindung eine Wählverbindung zum Verbindungspartner aufgebaut.

7.2.3 LAN-Schnittstelle zur Nutzung von ADSL konfigurieren (PPP-over-Ethernet)

ADSL Um mit **X4000** ADSL (Asymmetric Digital Subscriber Line) nutzen zu können, müssen Sie über die LAN-Schnittstelle ein PPP-over-Ethernet-Interface konfigurieren. Verbinden Sie dazu **X4000** mit T-DSL, dem ADSL-Anschluß der Deutschen Telekom AG.



Wenn Sie den ADSL-Anschluß eines anderen Providers nutzen, erkundigen Sie sich gegebenenfalls beim Provider über die zu beachtenden Besonderheiten Ihres ADSL-Anschlusses.

T-DSL Das T-DSL-Paket, das derzeit von der Deutschen Telekom AG als Hochgeschwindigkeitszugang zum Internet angeboten wird, besteht aus einem ISDN-Anschluß und einer Datenleitung mit einer Bandbreite von bis zu 768 kBit/s vom Internet Service Provider zum Kunden (downstream) und 128 kBit/s in Gegenrichtung (upstream).

Sicherheitsrisiken und Einschränkungen



Wenn die **X4000**-Anbindung an T-DSL nur über eine Ethernet-Schnittstelle erfolgt, ergeben sich folgende Einschränkungen und Sicherheitsrisiken:

- Beim Betreiben von PPP-over-Ethernet mit nur einer Ethernet-Schnittstelle ist die Gefahr von unberechtigten Zugriffen aus dem Internet auf das lokale **X4000**-LAN nicht auszuschließen. Solche unberechtigten Zugriffe können ihren Ursprung im ersten Knoten des Internets haben.
- Benutzer des lokalen Netzwerks können sich an ihrem PC einen PPP-over-Ethernet-Client einrichten und so, unbemerkt von **X4000**, das Internet nutzen.
- Broadcasts im lokalen LAN werden durch das ADSL-Modem (NTBBA) in jedem Fall zur Vermittlungsstelle der Telekom weitergeleitet und erst dort verworfen. Dadurch steht die maximale Bandbreite von 128 kBit/s upstream zur Telekom unter Umständen nicht vollständig zur Verfügung.

Die hier beschriebenen Einschränkungen und Sicherheitsrisiken entfallen, wenn **X4000** mit einer LAN-Erweiterungskarte ausgestattet ist und damit mehrere LAN-Schnittstellen zur Verfügung stehen (siehe [Kapitel 9.3.2, Seite 299](#)).

Der T-DSL-Anschluß (ohne **X4000**) sieht folgendermaßen aus:

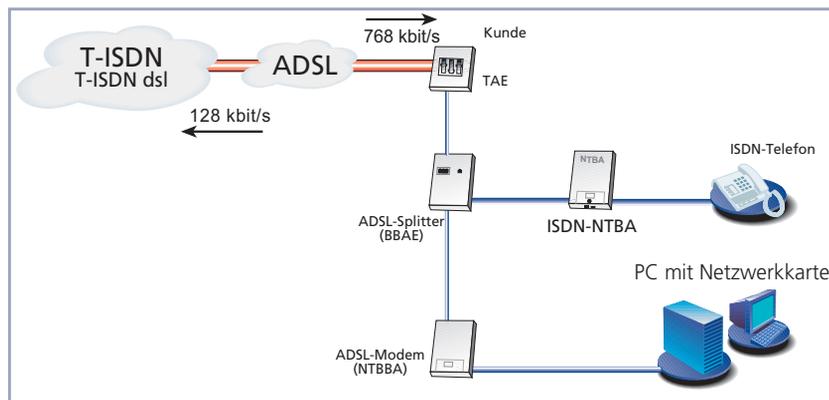


Bild 7-4: T-DSL-Anschluß (ohne **X4000**)

Das folgende Szenario (siehe [Bild 7-5, Seite 159](#)) dient zur Darstellung der erforderlichen Konfigurationsschritte: Die LAN-Schnittstelle von **X4000** ist, wie in

[Kapitel 3.3, Seite 59](#) beschrieben, mit Ihrem Hub verbunden, ebenso das ADSL-Modem (NTBBA) der Deutschen Telekom AG.



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

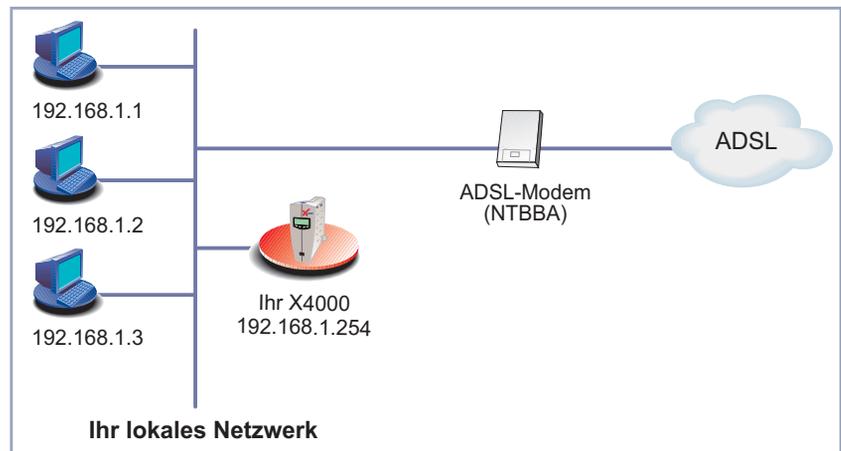


Bild 7-5: Beispielszenario (mit **X4000**)

Folgende Einstellungen sind erforderlich (die betroffenen Setup-Tool-Menüs sind an anderer Stelle beschrieben):

- Gehen Sie zu **PPP** (siehe [Kapitel 8.1.3, Seite 200](#)).
- Wählen Sie **PPPoE Ethernet Interface** aus: *en1*.
- Bestätigen Sie mit **SAVE**.
- Gehen Sie zu **WAN PARTNER** ➤ **ADD** (siehe [Tabelle 7-13, Seite 167](#)).
- Geben Sie **Partner Name** ein: z. B. *t-online*.
- Wählen Sie **Encapsulation** aus: *PPP*.
- Gehen Sie zu **WAN PARTNER** ➤ **ADD** ➤ **PPP** (siehe [Tabelle 7-18, Seite 172](#)).



- Geben Sie **Local PPP ID** (= Ihr Benutzername) ein:
z. B. `000460004256091169386#0001@t-online.de`.

Die T-Online Benutzername setzt sich folgendermaßen zusammen:
 <Anschlußkennung><T-Online-Nummer>#<Mitbenutzernummer>@t-online.de
 Die Anschlußkennung ist 12-stellig, hier: `000460004256`.
 Die T-Online-Nummer ist die Rufnummer, hier: `091169386`.
 Die Mitbenutzernummer ist die vierstellig, hier: `0001`.
 Die T-Online-Nummer und die Mitbenutzernummer müssen durch # getrennt werden, wenn die T-Online-Nummer weniger als 12 Stellen hat.

- Geben Sie **PPP Password** (= Ihr T-Online Paßwort) ein.
- Wählen Sie **Keepalives** aus: *on*.
- Bestätigen Sie mit **OK**.
- Gehen Sie zu **WAN PARTNER** ➤ **ADD** ➤ **ADVANCED SETTINGS** (siehe [Kapitel 8.2.5, Seite 226](#)).
- Wählen Sie **Layer 1 Protocol** aus: *PPP over Ethernet (PPPoE)*.
- Bestätigen Sie mit **OK**.
- Gehen Sie zu **WAN PARTNER** ➤ **ADD** ➤ **IP** (siehe [Tabelle 7-21, Seite 178](#)).
- Wählen Sie **IP Transit Network** aus: *dynamic client*.
- Bestätigen Sie mit **SAVE**.
- Gehen Sie zu **IP** ➤ **ROUTING** ➤ **ADD** (siehe "[Routing-Eintrag erstellen](#)", [Seite 179](#)).
- Wählen Sie **Route Type** aus: *Default route*.
- Wählen Sie **Network** aus: *WAN without transit network*.
- Wählen Sie **Partner / Interface** aus: z. B. *t-online*.
- Geben Sie **Metric** ein: z. B. *1*.
- Bestätigen Sie mit **SAVE**.
- Gehen Sie zu **IP** ➤ **NETWORK ADDRESS TRANSLATION** (siehe "[Network Address Translation \(NAT\) aktivieren](#)", [Seite 185](#)).

- Wählen Sie das PPPoE-Interface aus, z. B. **t-online**, und bestätigen mit der **Eingabetaste**.
- Wählen Sie **Network Address Translation** aus: *on*.
- Bestätigen Sie mit **SAVE**.

7.3 WAN-Partner einrichten

Um mit **X4000** Verbindungen zu Netzwerken oder Hosts außerhalb Ihres LANs herstellen zu können, müssen Sie die gewünschten Verbindungspartner als WAN-Partner auf **X4000** einrichten. Dies gilt sowohl für ausgehende Verbindungen (**X4000** wählt sich bei einem WAN-Partner ein), als auch für eingehende Verbindungen (ein WAN-Partner wählt sich bei **X4000** 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 **X4000** 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.

Allgemein Im folgenden wird in [Kapitel 7.3.1, Seite 162](#) in allgemeiner Form die Vorgehensweise erläutert, um einen WAN-Partner auf **X4000** einzurichten oder zu editieren.

Beispiele In [Kapitel 7.3.2, Seite 187](#) sind einige häufig benötigte Konfigurationsbeispiele dargestellt.



Wenn Sie einen Internetzugang über CompuServe einrichten möchten, beachten Sie bitte "[Internetzugang über CompuServe](#)", [Seite 189](#).

7.3.1 Prinzipielle Vorgehensweise

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

- WAN-Partner eintragen:

- >> **Protokoll** (Enkapsulierung) festlegen.
- Rufnummer(n) eintragen.
- >> **PPP**-Einstellungen zur Authentisierung festlegen.
- >> **Shorthold** festlegen.
- IP-Konfiguration durchführen.

■ Routing-Eintrag erstellen

■ Network Address Translation (>> **NAT**) aktivieren (optional)

Los geht's:

WAN-Partner eintragen

WAN-Partner einrichten

Bevor Sie zur Tat schreiten, sollten Sie sich gegebenenfalls die dafür notwendigen Zugangsdaten, die Sie von Ihrem ISP oder System-Administrator erhalten haben, zurechtlegen (siehe [Kapitel 6.1, Seite 111](#)). Die Bezeichnungen können unter Umständen von Provider zu Provider leicht variieren.

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

➤ Gehen Sie zu **WAN PARTNER:**

```

X4000 Setup Tool                               BinTec Communications AG
[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

```

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



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:

- *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

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

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

Ein weiteres Menüfenster erscheint:

X4000 Setup Tool	BinTec Communications AG
[WAN][ADD]:Configure WAN Partner	MyRouter
Partner Name	LittleIndian
Encapsulation	PPP
Compression	none
Encryption	none
Calling Line Identification	no
WAN Numbers >	
PPP >	
Advanced Settings >	
IP >	
IPX >	
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	<p> >> Enkapsulierung. Definiert, wie die >> Daten-Pakete für die Übertragung zum WAN-Partner verpackt werden. Mögliche Werte: </p> <ul style="list-style-type: none"> <input type="checkbox"/> <i>PPP</i> <input type="checkbox"/> <i>Multi-Protocol LAPB Framing</i> <input type="checkbox"/> <i>Multi-Protocol HDLC Framing</i> <input type="checkbox"/> <i>Async PPP over X.75</i> <input type="checkbox"/> <i>Async PPP over X.75/T.70/BTX</i> <input type="checkbox"/> <i>X.25_PPP</i> <input type="checkbox"/> <i>X.25</i> <input type="checkbox"/> <i>HDLC Framing (only IP)</i> <input type="checkbox"/> <i>LAPB Framing (only IP)</i> <input type="checkbox"/> <i>X31 B-Channel</i> <input type="checkbox"/> <i>X.25 No Signalling</i> <input type="checkbox"/> <i>X.25 PAD</i> <input type="checkbox"/> <i>X.25 No Configuration</i> <input type="checkbox"/> <i>Frame Relay</i> <input type="checkbox"/> <i>X.25 No Configuration, No Signalling</i>

Feld	Bedeutung
Compression	<p>Legt die Art der Komprimierung fest, die für den Datenverkehr mit dem WAN-Partner angewendet werden soll. Mögliche Werte:</p> <ul style="list-style-type: none"> ■ <i>STAC</i>: nur bei Encapsulation = PPP ■ <i>MS-STAC</i>: nur bei Encapsulation = PPP ■ <i>none</i>
Encryption	<p>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:</p> <ul style="list-style-type: none"> ■ <i>MPPE 40</i>: MPPE Version 1 mit 40-Bit-Schlüssel ■ <i>MPPE 56</i>: MPPE Version 1 mit 56-Bit-Schlüssel ■ <i>MPPE V2 40</i>: MPPE Version 2 mit 40-Bit-Schlüssel ■ <i>MPPE V2 56</i>: MPPE Version 2 mit 56-Bit-Schlüssel ■ <i>DES 56</i>: DES mit 56-Bit-Schlüssel ■ <i>Blowfish 56</i>: Blowfish mit 56-Bit-Schlüssel ■ <i>none</i>: keine Verschlüsselung <p>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.</p>

Feld	Bedeutung
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 7-13: **WAN PARTNER** ➤ **ADD**

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

Protokolle		Encapsulierung	Komprimierung: STAC, MS-STAC
IP	IPX		
X	X	<i>PPP</i>	X
X	X	<i>Async PPP over X.75</i>	X
X	X	<i>Async PPP over X.75/T.70/BTX</i>	X
X	X	<i>Multi-Protocol LAPB Framing</i>	
X	X	<i>Multi-Protocol HDLC Framing</i>	
X		<i>HDLC Framing (only IP)</i>	
X		<i>LAPB Framing (only IP)</i>	

Tabelle 7-14: Encapsulierung und Komprimierung

ToDo Machen Sie folgende Eintragungen:

- 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*.
- Gehen Sie zu **WAN PARTNER** ➤ **ADD** ➤ **WAN NUMBERS**:

Rufnummern eintragen

X4000 Setup Tool	BinTec Communications AG				
[WAN][ADD][WAN Numbers]: WAN Numbers (BigBoss)	MyRouter				
<p>WAN Numbers for this partner:</p> <table> <thead> <tr> <th>WAN Number</th> <th>Direction</th> </tr> </thead> <tbody> <tr> <td>0911987654321</td> <td>outgoing</td> </tr> </tbody> </table>		WAN Number	Direction	0911987654321	outgoing
WAN Number	Direction				
0911987654321	outgoing				
ADD	DELETE				
	EXIT				
Press<Ctrl-n>,<Ctrl-p>to scroll,<Space>tag/untag DELETE,<Return>toedit					

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

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

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

Ein weiteres Menüfenster erscheint:

X4000 Setup Tool	BinTec Communications AG						
[WAN][ADD][WANNUMBERS][ADD]:Add or Change WANNumbers(BigBoss)	MyRouter						
<table> <tbody> <tr> <td>Number</td> <td>0911987654321</td> </tr> <tr> <td>Direction</td> <td>outgoing</td> </tr> <tr> <td>Advanced Settings</td> <td>></td> </tr> </tbody> </table>	Number	0911987654321	Direction	outgoing	Advanced Settings	>	
Number	0911987654321						
Direction	outgoing						
Advanced Settings	>						
SAVE	Cancel						
Enter string, max length = 40 chars							

Das Menü enthält folgende Felder:

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

Tabelle 7-15: **WAN PARTNER** ► **ADD** ► **WAN NUMBERS** ► **ADD**

Das Feld **Direction** enthält folgende Auswahlmöglichkeiten:

Mögliche Werte	Bedeutung
<i>outgoing</i>	Für ausgehende Rufe, wenn Sie sich beim WAN-Partner einwählen wollen.
<i>both (CLID)</i>	Für eingehende und ausgehende Rufe.
<i>incoming (CLID)</i>	Für eingehende Rufe, wenn der WAN-Partner sich bei X4000 einwählen soll.

Tabelle 7-16: **Direction**



Wenn **X4000** an eine TK-Anlage angeschlossen ist, bei der für eine Amtsholung eine führende "0" gewählt wird, müssen Sie diese führende Null bei der Einwahlnummer berücksichtigen.

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

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

Wildcard	Bedeutung		Beispiel		
	Eingehende Rufe	Ausgehende Rufe	Number	X4000 akzeptiert eingehende Rufe z. B. mit:	Ausgehende Rufe, d. h. X4000 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	00123 und 123	00123

Tabelle 7-17: Wildcards für ein- und ausgehende Rufe



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

ToDo Machen Sie die folgenden Eintragungen:

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

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

Wenn ein Ruf eingeht, wird über den ISDN-➤➤ **D-Kanal** die Nummer des Anrufers mitgegeben. Anhand dieser Nummer kann **X4000** 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 System-Administrator der Firmenzentrale. Nur wenn diese Daten, die Sie auf **X4000** hier eintragen, mit den Daten des Anrufers übereinstimmen, wird der Ruf angenommen.

Wenn Sie WAN-Partner über einen RADISU-Server authentisieren, beachten Sie bitte die entsprechenden Hinweise in der [Extended Features Reference](#).

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

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

X4000 Setup Tool		BinTec Communications AG
[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	X4000s Kennung.
PPP Password	Paßwort.
Keepalives	Aktiviert Keepalive-Pakete zur Überprüfung des Interface-Status. Mögliche Werte: <input type="checkbox"/> <i>off</i> <input type="checkbox"/> <i>on</i>
Link Quality Monitoring	Aktiviert PPP Link Quality Monitoring nach RFC 1989. Mögliche Werte: <input type="checkbox"/> <i>off</i> <input type="checkbox"/> <i>on</i>

Tabelle 7-18: **WAN PARTNER** ➤ **ADD** ➤ **PPP**

Das Feld **Authentication** enthält folgende Auswahlmöglichkeiten:

Mögliche Werte	Bedeutung
<i>PAP</i>	Nur ►► PAP (PPP Password Authentication Protocol) ausführen, Paßwort wird unverschlüsselt übertragen.
<i>CHAP</i>	Nur ►► CHAP (PPP Challenge Handshake Authentication Protocol nach RFC 1994) ausführen, Paßwort wird verschlüsselt übertragen.
<i>CHAP + PAP</i>	Vorrangig CHAP, sonst PAP ausführen.
<i>MS-CHAP</i>	Nur MS-CHAP (MS Challenge Handshake Authentication Protocol) ausführen.
<i>CHAP + PAP + MS-CHAP</i>	Vorrangig CHAP ausführen, bei Ablehnung anschließend das vom WAN-Partner geforderte Authentisierungsprotokoll ausführen.
<i>MS-CHAP V2</i>	Nur MS-CHAP Version 2 ausführen.
<i>none</i>	Kein PPP-Authentisierungsprotokoll ausführen.

Tabelle 7-19: **Authentication**

ToDo Machen Sie folgende Eintragungen:

- 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 "[Paßwortänderung](#)", [Seite 85](#) 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 **X4000** nicht, welches Authentisierungsprotokoll mit diesem WAN-Partner festgelegt ist. Damit der Ruf trotzdem angenommen werden kann, greift **X4000** auf allgemeine Einstellungen im PPP zurück, die Sie nach Bedarf verändern können (siehe [Kapitel 8.1.3, Seite 200](#)).

Shorthold festlegen

Stellen Sie als nächstes Shorthold ein, um Gebühren zu sparen. **X4000** bricht dann die ISDN-Verbindung ab, wenn keine Daten mehr fließen. Mit statischem bzw. dynamischem Shorthold legen Sie fest, nach welchem Inaktivitätsintervall (Idle Timer) **X4000** die ISDN-Verbindung abbauen soll.

Statisch

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

Dynamisch

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

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



Bitte beachten Sie: dynamischen Shorthold können Sie nur nutzen, wenn Sie die 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 Dauer **➤➤ wähilverbindung** zu haben.

Dabei sollten Sie darauf achten, daß der statische Shorthold später einsetzt als der dynamische. Andernfalls beendet **X4000** die Verbindung immer gemäß dem statischen Shorthold, der dynamische Shorthold kann nicht greifen. Geben Sie deshalb in diesem Fall als **Static Short Hold (sec)** einen Wert ein, der etwas über dem maximal zu erwartenden dynamischen Inaktivitätsintervall liegt.

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

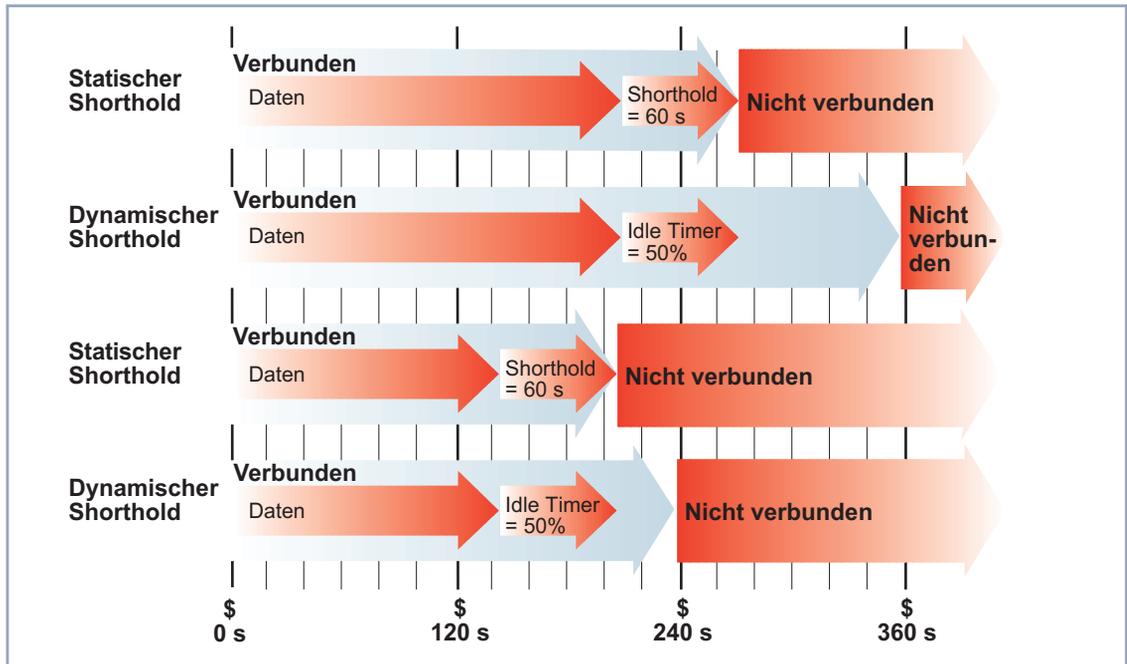


Bild 7-6: Dynamischer und statischer Shorthold

Gehen Sie folgendermaßen vor:

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

X4000 Setup Tool		BinTec Communications AG	
[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 Teile des Menüs sind für diesen Konfigurationsschritt relevant:

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

Tabelle 7-20: **WAN PARTNER** ➤ **ADD** ➤ **ADVANCED SETTINGS**

ToDo Machen Sie folgende Eintragungen:

- Geben Sie **Static Short Hold (sec)** ein, z. B. 20.
- Geben Sie **Idle for Dynamic Short Hold (%)** ein, z. B. 0.

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



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

- Für interaktive Verbindungen (z. B. ➤➤ **telnet**) sollten Sie einen hohen Wert eingeben (z. B. 80...90), um Verbindungsabbrüche während kurzer Phasen ohne Datenfluß zu vermeiden.
- Für Internet-Verbindungen (z. B. WWW, http, usw.) sollten Sie einen mittleren bis hohen Wert eingeben (z. B. 50...80), um Verbindungsabbrüche während Wartephases 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**.

X4000 Setup Tool		BinTec Communications AG
[WAN][ADD][IP]: IP Configuration (BigBoss)		MyRouter
IP Transit Network		no
Partner's LAN IP Address		10.1.1.0
Partner's LAN Netmask		255.255.255.0
Advanced Settings >		
	SAVE	CANCEL
Use <Space> to select		

Das Menü enthält folgende Felder:

Feld	Bedeutung
IP Transit Network	Legt fest, ob X4000 ein Transit Network zum WAN-Partner aufbaut.
local IP Address	IP-Adresse von X4000 . Im Normalfall müssen Sie hier keinen Eintrag machen, außer Sie richten für einen Ihrer WAN-Partner ein Transit-network ein (siehe Kapitel 8.2.6, Seite 229).
local ISDN IP Address	ISDN-IP-Adresse von X4000 im Transit Network.
Partner's ISDN IP Address	ISDN-IP-Adresse des WAN-Partners im Transit Network.
Partner's LAN IP Address	IP-Adresse des LAN des WAN-Partners.
Partner's LAN Netmask	Netzmaske des LAN des WAN-Partners. Wenn Sie keinen Eintrag machen, trägt X4000 eine Standard-Netzmaske für die unter <i>Partner's LAN IP Address</i> verwendete Netzklasse ein.

Tabelle 7-21: **WAN PARTNER** ➤ **ADD** ➤ **IP**

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

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

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



Wenn Sie einen Internetzugang einrichten, kennen Sie normalerweise die IP-Adresse Ihres Internet Service Providers (ISP) nicht und **X4000** bekommt die **local ISDN IP Address** dynamisch (für die Dauer der Verbindung) oder statisch vom ISP zugewiesen. Machen Sie in diesem Fall folgende Einstellungen in **WAN PARTNER ► ADD ► IP:**

- IP-Adresse wird dynamisch zugewiesen:
 - Wählen Sie **IP Transit Network** aus: *dynamic client*.
- IP-Adresse wird statisch zugewiesen:
 - Wählen Sie **IP Transit Network** aus: *yes*.
 - **Local ISDN IP Address: X4000s** 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 **X4000s** statische IP-Adresse, die Sie vom ISP erhalten.
 - Keine Eintragungen für **Partner's LAN IP Address** und **Partner's LAN Netmask**.

Wenn Sie mehr wissen wollen, z. B. was ein Transit Network eigentlich ist und wofür Sie es brauchen, siehe [Kapitel 8.2.6, Seite 229](#).



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

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

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

Routing-Eintrag erstellen

Routing-Eintrag erstellen

Sie haben jetzt einen WAN-Partner auf **X4000** eingetragen. Für jeden WAN-Partner wird automatisch ein Routing-Eintrag in der Routing-Tabelle von **X4000** erzeugt. Die Routing-Einträge können Sie ändern und weitere hinzufügen. Für die Verbindung zu Ihrem Internet Service Provider sollten Sie immer eine sog. Default-Route einrichten.

Gehen Sie folgendermaßen vor:

➤ Gehen Sie zu **IP** ➤ **ROUTING**:

X4000 Setup Tool		BinTec Communications AG				
[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	255.255.255.0	US	0	en1	loc
10.1.1.0		255.255.255.0	DI	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						

Hier sind alle eingetragenen IP-Routen aufgelistet. Unter **Flags** wird der aktuelle Status (Up – Aktiv, Dormant – Ruhend, Blocked – Gesperrt) und die Art der Route (Gateway Route, Interface Route, Subnet Route, Host Route, Extended Route) angezeigt. Unter **Pro** wird angezeigt, mit welchem Protokoll **X4000** den Routing-Eintrag "gelernt" hat.

Gehen Sie folgendermaßen vor, um eine Route festzulegen:

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

Ein weiteres Menüfenster erscheint:



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 10.2.12, Seite 368](#).

X4000 Setup Tool		BinTec Communications AG	
[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: <ul style="list-style-type: none"> ■ <i>Host route</i>: Route zu einem einzelnen Host ■ <i>Network route</i>: Route zu einem Netzwerk ■ <i>Default route</i>: Wird nur benutzt, wenn keine andere passende Route verfügbar ist
Network	Definiert die Art der Verbindung (LAN, WAN), siehe Tabelle 7-23, Seite 183 .
Destination IP-Address	IP-Adresse des Ziel-Hosts oder -LANs.
Netmask	Netzmaske des Partner-LANs (nur möglich bei Route Type = <i>Network route</i> . Wenn keine Eintragung gemacht wird, benutzt der Router eine Standardnetzmaske).
Partner / Interface	WAN-Partner (nur möglich bei Network = <i>WAN without transit network</i>)
Gateway IP-Address	IP-Adresse des Hosts, an den X4000 die IP-Pakete weitergeben soll.
Metric	Je niedriger der Wert, desto höhere Priorität besitzt die Route. (Wertebereich 1...14)

Tabelle 7-22: **IP** ➤ **ROUTING** ➤ **ADD**

Das Feld **Network** enthält folgende Auswahlmöglichkeiten:

Mögliche Werte	Bedeutung
<i>LAN</i>	Route zu einem Ziel-Host oder -LAN, das über X4000 s LAN-Anschluß zu erreichen ist.
<i>WAN without transit network</i>	Route zu einem Ziel-Host oder -LAN, das über einen WAN-Partner ohne Transit Network zu erreichen ist.
<i>WAN with transit network</i>	Route zu einem Ziel-Host oder -LAN, das über einen WAN-Partner mit Transit Network zu erreichen ist.
<i>Refuse</i>	X4000 verwirft Datenpakete, die diese Route benutzen, und übermittelt dem Absender eine Meldung, daß das Ziel des Paketes unerreichbar ist.
<i>Ignore</i>	X4000 verwirft Datenpakete, die diese Route benutzen, ohne eine Statusmeldung zu senden.

Tabelle 7-23: **Network**



Sie können auf **X4000** nur eine einzige Default-Route eintragen: Wenn Sie also einen Zugang zum Internet einrichten, dann tragen Sie die Route zu Ihrem Internet Service Provider (ISP) als Default-Route ein.

Wenn Sie 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 **X4000** 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 gespeichert, 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 Sub-Netz, das Sie in diesem Netzwerk erreichen wollen, einen eigenen Routing-Eintrag vornehmen.

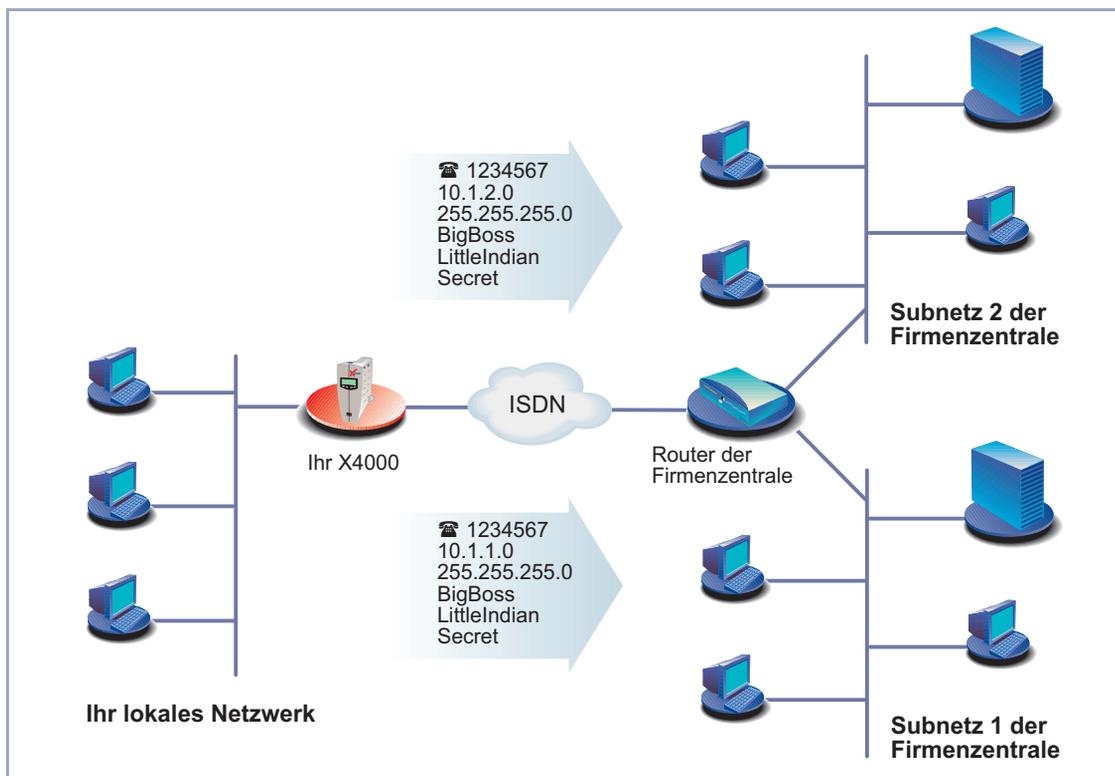


Bild 7-7: Netzwerk mit Subnetzen

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

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

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

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

Network Address Translation (NAT) aktivieren

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

Detaillierte Informationen zu Network Address Translation (NAT) finden Sie in [Kapitel 10.2.7, Seite 344](#).

Gehen Sie folgendermaßen vor, um NAT zu aktivieren:

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

```

X4000 Setup Tool                               BinTec Communications AG
[IP][NAT]: NAT Configuration                     MyRouter

Select IP Interface to be configured for NAT

                                Nat          static mappings
GoInternet                       on           2
LittleIndian                     off
enl                              off
enl-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 erscheint:

```

X4000 Setup Tool                               BinTec Communications AG
[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 Machen Sie folgende Eintragungen:

- Wählen Sie **Network Address Translation** aus: *on*.
- Bestätigen Sie mit **SAVE**.
Network Address Translation ist für die ausgewählte Schnittstelle bzw. den ausgewählten WAN-Partner aktiviert.
- Verlassen Sie **IP** ➤ **NETWORK ADDRESS TRANSLATION** mit **EXIT**.

- Verlassen Sie **IP** mit **EXIT**.

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

Um trotz aktiviertem NAT bestimmte Verbindungen von außen zu Hosts innerhalb des LANs zu erlauben, müssen Sie die erlaubten Sessions genau definieren. Wie Sie dabei vorgehen finden Sie in [Kapitel 10.2.7, Seite 344](#).

7.3.2 Beispiele

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

- ["Internetzugang über T-Online", Seite 187](#)
- ["Internetzugang über Compuserve", Seite 189](#)



Die Vorgehensweise bei der Eingabe von Paßwörtern ist unter "[Paßwortänderung](#)", [Seite 85](#) beschrieben.

Internetzugang über T-Online

T-Online Folgende Einstellungen sind erforderlich:

- In **WAN PARTNER** ➤ **ADD**:
Partner Name: z. B. *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: z. B. *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** ►
Eingabetaste:
 - Network Address Translation:** *on*

7.4 Konfigurationsdatei sichern

Nachdem Sie nun auf **X4000** eine funktionierende Konfiguration erstellt haben, sollten Sie diese sichern:

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

Ein weiteres Menüfenster erscheint:

```
X4000 Setup Tool                               BinTec Communications AG
[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 erscheint die SNMP-Shell von **X4000** mit dem Login-Prompt. Alle Änderungen, die Sie vorher mit dem Setup Tool durchgeführt haben, sind gesichert. Beim nächsten Starten von **X4000** wird die so abgespeicherte Konfigurationsdatei geladen.
- Wählen Sie **Exit without saving**, um das Setup Tool zu verlassen, die vorgenommenen Änderungen aber nicht zu speichern.
Es erscheint die SNMP-Shell von **X4000** mit dem Login-Prompt. Alle Änderungen, die Sie vorher mit dem Setup Tool durchgeführt haben, gehen beim Ausschalten von **X4000** verloren.

8 Weiterführende Konfiguration des Grundgeräts mit dem Setup Tool

In diesem Kapitel finden Sie weitere Möglichkeiten zur Konfiguration von **X4000** für den fortgeschrittenen Benutzer. Wenn Sie zusätzliche Einstellungen machen wollen, die mit dem Configuration Wizard bzw. dem [Kapitel 6, Seite 123](#) nicht abgedeckt werden, dann sind Sie hier richtig.

Folgende Konfigurationsschritte werden erläutert:

- Allgemeine >> **WAN**-Einstellungen ([Kapitel 8.1, Seite 194](#))
- WAN-Partner-spezifische Einstellungen ([Kapitel 8.2, Seite 204](#))
- Grundlegende >> **IP**-Einstellungen ([Kapitel 8.3, Seite 249](#))
- >> **IPX**-Einstellungen ([Kapitel 8.4, Seite 278](#))
- Bridging ([Kapitel 8.5, Seite 285](#))
- Funktionen mit Zusatzlizenz ([Kapitel 8.6, Seite 286](#))



Nutzen Sie die Funktion Taschengeldkonto (siehe [Kapitel 10.1.3, Seite 328](#)). Damit können Sie für Verbindungen mit **X4000** ein Limit festlegen, um Gebühren aufgrund von Fehlern bei der Konfiguration in Grenzen zu halten.

8.1 Allgemeine WAN-Einstellungen

Allgemeine WAN-Funktionen:

- **X4000** als dynamischer IP-Adreß-➤➤ **Server** ([Kapitel 8.1.1, Seite 194](#))
- CAPI User Concept ([Kapitel 8.1.2, Seite 196](#))
- Allgemeine ➤➤ **PPP**-Einstellungen ([Kapitel 8.1.3, Seite 200](#))
- Einstellung des X.31-TEI-Werts ([Kapitel 8.1.4, Seite 203](#))

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

8.1.1 Dynamic IP Address Server

IP-Adreß-Pools **X4000** kann als dynamischer IP-Adreß-Server für PPP-Verbindungen agieren. Dafür stellen Sie einen oder mehrere Pools von ➤➤ **IP-Adressen** zur Verfügung. Diese IP-Adressen können für die Dauer der Verbindung an einwählende WAN-Partner vergeben werden.



Eingetragene Host-Routen haben immer Vorrang vor IP-Adressen aus den Adreß-Pools. D. h. wenn ein eingehender Ruf authentisiert wurde, überprüft **X4000** zunächst, ob für den Anrufer in der Routing-Tabelle eine Host-Route eingetragen ist. Wenn dies nicht der Fall ist, kann **X4000** eine IP-Adresse aus einem Adreß-Pool zuweisen (falls verfügbar).



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

Die Konfiguration erfolgt in:

- **IP** ➤ **IP ADDRESS POOL WAN (PPP)**
- **WAN PARTNER** ➤ **EDIT** ➤ **IP**
- **WAN PARTNER** ➤ **EDIT** ➤ **IP** ➤ **ADVANCED SETTINGS**

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

Tabelle 8-1: **IP ► IP ADDRESS POOL WAN (PPP)**

Feld	Bedeutung
IP Transit Network	Legt fest, ob zwischen X4000 und WAN-Partner ein Transit-Netzwerk verwendet werden soll. Bei Zuweisung eines Adreß-Pools muß hier <i>dynamic server</i> ausgewählt werden.

Tabelle 8-2: **WAN PARTNER ► EDIT ► IP**

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

Tabelle 8-3: **WAN PARTNER ► EDIT ► IP ► ADVANCED SETTINGS**

ToDo Gehen Sie folgendermaßen vor:

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

8.1.2 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 **X4000** nutzen können.

Beispiel Damit wird z. B. ermöglicht, daß ein eingehendes Fax an den Benutzer Winnetou auch wirklich nur an den Benutzer Winnetou und nicht etwa 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 142), werden alle eingehenden Rufe, die an den Dienst CAPI weitergeleitet werden, allen CAPI-Applikationen im LAN angeboten. Und wer am schnellsten reagiert, erhält den Ruf. Wenn OldShatterhand also schneller ist...

Die Konfiguration erfolgt in:

- **CAPI** ➤ **USER**
- **CM-1BRI, ISDN S0** ➤ **INCOMING CALL ANSWERING**

Feld	Bedeutung
Name	Benutzername, für den 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: <ul style="list-style-type: none">■ <i>enabled</i>: Zugriff auf CAPI erlaubt■ <i>disabled</i>: Zugriff auf CAPI gesperrt

Tabelle 8-4: CAPI ➔ USER

Feld	Bedeutung
Item	Dienst, der einen Ruf auf die untenstehende Number annehmen soll.
Number	Rufnummer, unter der der oben eingetragene Dienst (Item) erreicht werden kann.
Mode	Modus, mit dem X4000 den Ziffernvergleich von Number mit der Called Party Number des eingehenden Rufes durchführt: <i>right to left</i> : Dies ist der Standard. <i>left to right (DDI)</i> : Immer dann auswählen, wenn X4000 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.
Bearer	Art des eingehenden Rufes. Mögliche Werte: <input type="checkbox"/> <i>data</i> : Daten-Ruf <input type="checkbox"/> <i>voice</i> : Sprach-Ruf <input type="checkbox"/> <i>any</i> : beliebiger Ruf

Tabelle 8-5: **CM-1BRI, ISDN S0** ➔ **INCOMING CALL ANSWERING**

Wenn sich beim Starten von **X4000** in **CAPI** ➔ **USER** kein Eintrag befindet, wird automatisch ein Standard-Eintrag ohne Paßwort erzeugt (mit **Name** = *default* und **CAPI** = *enabled*).

ToDo Gehen Sie folgendermaßen vor:

- Gehen Sie zu **CAPI** ➔ **USER**.
- Wählen Sie einen bestehenden Eintrag aus und bestätigen Sie mit der **Eingabetaste** oder fügen Sie einen neuen Eintrag mit **ADD** hinzu.
- Geben Sie **Name** ein.



- Geben Sie **Password** ein.

Die Vorgehensweise bei der Eingabe von Paßwörtern im Setup Tool ist unter "[Paßwortänderung](#)", Seite 85 beschrieben.

- Wählen Sie **CAPI** aus.
- Bestätigen Sie mit **SAVE**.
- Wiederholen Sie diese Schritte für jeden Benutzer im LAN.
- Gehen Sie zu **CM-1BRI, ISDN SO** ➤ **INCOMING CALL ANSWERING**.
Machen Sie hier für jeden Benutzer im LAN, der Zugriff auf den Dienst CAPI hat, einen Eintrag.
- Wählen Sie einen bestehenden Eintrag aus und bestätigen Sie mit der **Ein- gabetaste** 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 **X4000** 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, d.h. es genügt ein einziger Eintrag.

Sie sollten auf jeden Fall versuchen, Ihr Rechnersystem auf CAPI 2.0 umzu- stellen, 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 so oft, bis Sie für jeden Nutzer einen Eintrag erstellt haben.



Bei der Remote-CAPI-Konfiguration auf den Hosts müssen Sie dann für jeden Benutzer jeweils Benutzernamen und Paßwort eintragen, entsprechend den Eintragungen auf **X4000**.

8.1.3 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 7.3, Seite 162](#)). Wenn ein Ruf eingeht, erkennt **X4000** 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 manchen Fällen kann ein eingehender Ruf aber nicht via CLID identifiziert werden. Dies ist z. B. dann der Fall,

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

In beiden Fällen kommt bei **X4000** keine Calling Line Number an. Eine Identifizierung des Anrufers via CLID kann also nicht erfolgen, auch wenn der Anrufer als WAN-Partner eingetragen ist. **X4000** weiß nicht, mit welchem ➤➤ **PPP-Authentisierungsprotokoll** er den eingehenden Ruf identifizieren kann.

Allgemeine PPP-Einstellungen Um eine Rufannahme trotzdem zu ermöglichen, führt **X4000** 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 **X4000** den ankommenden Ruf.

Die Konfiguration der allgemeinen PPP-Einstellungen erfolgt in **PPP**:

Feld	Bedeutung
Authentication Protocol	<p>Definiert das PPP-Authentisierungs-Protokoll, das dem Anrufer als erstes angeboten wird. Mögliche Werte:</p> <ul style="list-style-type: none"> ■ <i>PAP</i>: nur PAP ■ <i>CHAP</i>: nur CHAP ■ <i>CHAP + PAP</i>: erst CHAP, dann PAP ■ <i>MS-CHAP</i>: nur MS-CHAP ■ <i>CHAP + PAP + MS-CHAP</i>: erst CHAP, bei Ablehnung anschließend das vom Anrufer gewollte Protokoll ■ <i>MS-CHAP V2</i>: nur MS-CHAP Version 2 ■ <i>none</i>: keine PPP-Authentisierung
Radius Server Authentication	<p>Einstellungen zur RADIUS Server Authentisierung. Zu RADIUS siehe Extended Features Reference.</p>
PPP Link Quality Monitoring	<p>Definiert, ob Link Quality Monitoring für PPP-Verbindungen durchgeführt wird. Mögliche Werte:</p> <ul style="list-style-type: none"> ■ <i>no</i>, wird nicht durchgeführt. ■ <i>yes</i>, die Verbindungsstatistiken werden in der ➤➤ MIB-Tabelle biboPPPLQMTTable gespeichert.
PPPoE Ethernet Interface	<p>Definiert das Interface, über welches PPP-over-Ethernet zur Nutzung eines ADSL-Anschlusses läuft (siehe Kapitel 7.2.3, Seite 157).</p>

Tabelle 8-6: **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**.

8.1.4 X.31 TEI

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 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 <i>specify</i> gesetzt. Hat die Autokonfiguration den TEI nicht erkannt, können Sie hier manuell <i>specify</i> 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.
X.31 TEI Service	Hier wählen Sie den Service, für den Sie den X.31-TEI nutzen wollen. Mögliche Werte: <ul style="list-style-type: none"> ■ <i>Capi</i> ■ <i>Capi Default</i> ■ <i>Packet Switch</i> <i>Capi</i> und <i>Capi Default</i> dienen zur Nutzung des X.31-TEI für CAPI-Applikationen. Bei <i>CAPI</i> wird der in der CAPI-Applikation eingestellte TEI-Wert benutzt, bei <i>Capi Default</i> wird der Wert der CAPI-Applikation ignoriert und immer der hier eingestellte Standardwert benutzt. <i>Packet Switch</i> stellen Sie ein, wenn Sie die X.31-TEI für den X.25-Router nutzen möchten.

Tabelle 8-7: **CM-1BRI, ISDN S0** ► **ADVANCED SETTINGS**

8.2 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 8.2.1, Seite 204](#))
- Channel-Bundling ([Kapitel 8.2.2, Seite 205](#))
- Bandwidth on Demand (BoD) ([Kapitel 8.2.3, Seite 207](#))
- Always On/Dynamic ISDN (AO/DI) ([Kapitel 8.2.4, Seite 213](#))
- Layer 1 Protocol (ISDN-B-Kanal) ([Kapitel 8.2.5, Seite 226](#))
- IP Transit Network ([Kapitel 8.2.6, Seite 229](#))
- Übermittlung von DNS- und WINS-Server-IP-Adressen an WAN-Partner ([Kapitel 8.2.7, Seite 232](#))
- ►► **RIP** (Routing Information Protocol) ([Kapitel 8.2.8, Seite 236](#))
- Komprimierung: ►► **VJHC**, ►► **STAC**, MS-STAC ([Kapitel 8.2.9, Seite 239](#))
- ►► **Proxy ARP** (Address Resolution Protocol) ([Kapitel 8.2.10, Seite 241](#))
- Keepalive Monitoring ([Kapitel 8.2.11, Seite 243](#))

Im folgenden werden die jeweils erforderlichen Konfigurationsschritte genau erläutert.

8.2.1 Delay after Connection Failure

Mit dieser Funktion richten Sie eine Wartezeit nach fehlgeschlagenem Verbindungsversuch durch **X4000** 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 fehlgeschlagenem Verbindungsaufbau kein erneuter Versuch durch X4000 unternommen wird.

Tabelle 8-8: **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**.

8.2.2 Channel Bundling

X4000 unterstützt dynamische und statische ►► **Kanalbündelung** für Wählverbindungen. Bei Aufbau einer Verbindung wird zunächst nur ein B-Kanal geöffnet.

Dynamisch Dynamische Kanalbündelung bedeutet, daß **X4000** 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 **X4000** 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 ganzen Verbindung geöffnet sind.

Tabelle 8-9: **WAN PARTNER** ► **EDIT** ► **ADVANCED SETTINGS**

Das Feld **Channel-Bundling** enthält folgende Auswahlmöglichkeiten:

Mögliche Werte	Bedeutung
<i>no</i>	Keine Kanalbündelung, für Verbindungen steht immer nur ein B-Kanal zur Verfügung.
<i>dynamic</i>	Dynamische Kanalbündelung.
<i>static</i>	Statische Kanalbündelung.

Tabelle 8-10: **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**.

Beachten Sie auch die Funktion Bandwidth on Demand (BOD), siehe [Kapitel 8.2.3, Seite 207](#).

8.2.3 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 1 zusätzlicher Kanal erlaubt wurde (**Maximum Number of Dialup Channels** > 1).

Zu- und Abschalten von B-Kanälen

Ein B-Kanal wird zugeschaltet, wenn der aktuelle Durchsatz der entsprechenden Schnittstelle zum Verbindungspartner für mindestens 5 Sekunden 90% oder mehr des maximal möglichen Durchsatzes beträgt.

Für das Abschalten eines zugeschalteten B-Kanals ist nicht der aktuelle Durchsatz interessant, sondern der berechnete (also fiktive) Durchsatz des Kanalbündels nach Abschalten eines B-Kanals. Ein B-Kanal wird abgeschaltet, wenn der berechnete Wert 10 Sekunden lang unter 80% des maximal möglichen Durchsatzes der übrigbleibenden Kanäle bleibt.

Statischer oder dynamischer Short Hold können ebenso zum Abschalten eines zusätzlichen B-Kanals führen. Wenn statischer Short Hold konfiguriert wurde, hat dieser immer die höchste Priorität. Wenn dynamischer Short Hold konfiguriert wurde, muß zusätzlich der oben genannte berechnete Wert zutreffen.

X4000 unterstützt auch die Funktion AO/DI (Always On/Dynamic ISDN), um den ISDN-D-Kanal zur Datenübertragung zu nutzen (siehe [Kapitel 8.2.4, Seite 213](#)).

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 7.3, Seite 162](#))
- **WAN PARTNER** ► **EDIT** ► **PPP** (Beschreibung des Menüs in [Kapitel 7.3, Seite 162](#))

Das Menü **WAN PARTNER** ► **EDIT** ► **ADVANCED SETTINGS** ► **EXTENDED INTERFACE SETTINGS (OPTIONAL)** enthält folgende Felder:



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

Feld	Bedeutung
Mode	Legt fest, welcher Modus für BOD verwendet wird. Mögliche Werte: siehe Tabelle 8-12 , Seite 212 .
Line Utilization Weighting	Legt fest, wie die Auslastung der Verbindung berechnet wird. Mögliche Werte: <ul style="list-style-type: none"> ■ <i>equal</i>: Für die Berechnung werden alle gemessenen Werte für den Durchsatz innerhalb von Line Utilization Sample (sec) gleich gewichtet (Standardwert). ■ <i>proportional</i>: 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.
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 8.2.4 , Seite 213).

Feld	Bedeutung
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 8-11: **WAN PARTNER** ➤ **EDIT** ➤ **ADVANCED SETTINGS** ➤ **EXTENDED INTERFACE SETTINGS (OPTIONAL)**

Das Feld **Mode** enthält folgende Auswahlmöglichkeiten:

Mögliche Werte	Bedeutung
<i>Bandwidth On Demand Disabled</i>	Deaktiviert BOD, es werden keine zusätzlichen Kanäle geöffnet (Standardwert).
<i>Bandwidth On Demand Enabled</i>	(Nur bei Wählverbindungen) Aktiviert BOD, es können zusätzliche Kanäle geöffnet werden. Der Verbindungspartner, der die Verbindung initiiert hat, öffnet die zusätzlichen Kanäle.
<i>BAP, Active Mode</i>	(Erforderlich für die Funktion AO/DI (Always On/Dynamic ISDN), siehe Tabelle 8-17 , Seite 220)
<i>BAP, Passive Mode</i>	Wird derzeit von X4000 nicht unterstützt.
<i>BAP, Active and Passive Mode</i>	Wird derzeit von X4000 nicht unterstützt.
<i>BAP, Client Active Mode</i>	Wird derzeit von X4000 nicht unterstützt.
<i>Backup</i>	(Nur bei Festverbindungen) 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.
<i>Bandwidth On Demand Active</i>	(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.

Mögliche Werte	Bedeutung
<i>Bandwidth On Demand</i> <i>Passive</i>	(Nur bei Festverbindungen) Ermöglicht BOD und definiert den passiven Partner. Diese Seite aktiviert kein Zu- und Abschalten von zusätzlichen Kanälen.

Tabelle 8-12: **Mode**

ToDo Gehen Sie folgendermaßen vor:

- Gehen Sie zu **WAN PARTNER** ➤ **EDIT** ➤ **ADVANCED SETTINGS** ➤ **EXTENDED INTERFACE SETTINGS (OPTIONAL)**.
- Wählen Sie **Mode** und **Line Utilization Weighting** aus.
- Tragen Sie **Line Utilization Sample (sec)** und **Maximum Number of Dialup Channels** 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**.

8.2.4 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 Internet Service Provider dar.

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 zwei B-Kanäle dynamisch hinzugeschaltet (Dynamic ISDN). Die Datenübertragung erfolgt in diesem Fall ausschließlich im B-Kanal bzw. in den B-Kanälen, d.h. die B-Kanäle bleiben bandbreiten-intensiven Anwendungen vorbehalten (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 bandbreiten-intensive Anwendungen

Wie funktioniert AO/DI?

AO/DI wird bei **X4000** 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 es werden gegebenenfalls eine

dynamische IP-Adresse und DNS-Adressen zugewiesen (AO/DI-Client-Modus).

Die Verwendung der B-Kanäle wird anhand des Datendurchsatzes oder über applikationsabhängiges Bandbreitenmanagement (Bandwidth on Demand, BOD für IP-basierende Applikationen) geregelt. 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. 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 **X4000** ist dies durch eine erweiterte Konfigurationsmöglichkeit innerhalb des IP-Subsystems realisiert. Analog dem Konzept für IP-Access-Listen werden einem Interface Filter, Regeln und Regelketten zugewiesen (siehe Benutzerhandbuch, Kapitel 9.2.8 "Filter (Access Lists)". 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 **X4000** für AO/DI zu konfigurieren, sind folgende Schritte erforderlich:

- X.31-Konfiguration durchführen, d.h. den TEI (terminal endpoint identifier) Value für X.25 (Packet Switch) reservieren (siehe "[X.31-Konfiguration](#)", [Seite 215](#))
- X.25 Konfiguration durchführen (siehe "[X.25-Konfiguration](#)", [Seite 216](#)):
 - Link-Konfiguration für Datex-P
 - Call-Routing
- AO/DI-Partner als WAN-Partner anlegen (siehe "[AO/DI-Partner als WAN-Partner anlegen](#)", [Seite 217](#))

- 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

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 das Feld **Windowsize/ Packetsize Neg.** ausgeschaltet werden.

Bei **X4000** ist die X.25-Software grundsätzlich als X.25-Switch ausgelegt. Für AO/DI muß dieser Switch entsprechend konfiguriert werden (siehe "[X.25-Konfiguration](#)", Seite 216).

Im folgenden finden Sie alle notwendigen Schritte, um **X4000** 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 8.1.4, Seite 203](#)).
- Wählen Sie **X.31 TEI Value** aus: *specify*.



specify sollte der voreingestellte Wert für **X.31 TEI Value** 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: *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 Extended Features Reference auf www.bintec.de.

X.25-Konfiguration 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 Teile 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: <i>never</i> , d.h. die Aushandlung wird abgeschaltet.
Highest Two-Way-Channel (HTC)	Definiert die höchste Anzahl an virtuellen Kanälen.

Tabelle 8-13: **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 Teile 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 8-14: **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**.

Folgender Teil des Menüs ist für diesen Konfigurationsschritt relevant:

Feld	Bedeutung
Layer 1 Protocol	Legt fest, welches Layer 1 Protocol X4000 nutzen soll. Für AO/DI gibt es nur eine sinnvolle Einstellung: <i>AO/DI</i> .
Channel-Bundling	Legt fest, ob bzw. welche Art von Kanalbündelung für Verbindungen mit dem WAN-Partner genutzt werden soll (siehe Handbuch, Kapitel 7.2.2) Wenn unter Layer 1 Protocol <i>AO/DI</i> ausgewählt ist, ist für Channel-Bundling automatisch <i>dynamic</i> eingestellt.
Total Number of Channels	Definiert bei dynamischer Kanalbündelung die maximale Anzahl der Kanäle, die geöffnet werden dürfen.
Remote X.25 Address	X.25-Zieladresse. Erscheint nur, wenn unter Layer 1 Protocol <i>AO/DI</i> ausgewählt ist.

Tabelle 8-15: **WAN PARTNER** ➤ **ADD** ➤ **ADVANCED SETTINGS**

- Wählen Sie **Layer 1 Protocol** aus: *AO/DI*.
- Geben Sie **Total Number of Channels** ein, z. B. *1*.
- 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)**.

Folgender Teil des Menüs ist für diesen Konfigurationsschritt relevant:

Feld	Bedeutung
Mode	Legt fest, welcher Modus für BOD verwendet wird. Für AO/DI-Client wird ausschließlich die Einstellung <i>BAP, Active Mode</i> 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 8-16: **WAN PARTNER** ► **ADD** ► **ADVANCED SETTINGS** ► **EXTENDED INTERFACE SETTINGS (OPTIONAL)**

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

Mögliche Werte	Bedeutung
<i>BAP, Active Mode</i>	<p>Das Bandwidth Allocation Protocol (BAP) kennt drei verschiedene Möglichkeiten, eine Bandbreitenänderung zu vereinbaren. Im Active Mode zeigt es folgendes Verhalten:</p> <ul style="list-style-type: none"> ■ Call-Request: einer der beiden Kommunikationspartner möchte einen B-Kanal zuschalten; das Zuschalten wird gegebenenfalls initiiert. ■ 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 gegebenenfalls initiiert oder akzeptiert.

Tabelle 8-17: **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 Internet 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.

Applikationsgesteuertes Bandbreitenmanagement (optional)

Filter und Regeln

Applikationsgesteuertes Bandbreitenmanagement wird über Filter und Regeln in ähnlicher Weise konfiguriert wie Access-Listen für IP-Pakete (siehe [Kapitel 10.2.8, Seite 349](#)). 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**.

Eine Regel für BOD wird in ähnlicher Weise festgelegt wie eine Regel für IP-Pakete (siehe [Kapitel 10.2.8, Seite 349](#)). 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 10.2.8, Seite 349](#)) enthält das Menü folgende Felder:

Feld	Bedeutung
Direction	Richtung der Datenpakete, auf die die Regel angewandt werden soll. Mögliche Werte: <ul style="list-style-type: none"> ■ <i>incoming</i>: eingehende Datenpakete ■ <i>outgoing</i>: ausgehende Datenpakete ■ <i>both</i>: eingehende und ausgehende Datenpakete
Number of Channels	Zahl der B-Kanäle, die zugeschaltet werden sollen.

Tabelle 8-18: **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
<i>invoke M</i>	B-Kanäle werden zugeschaltet, wenn die Regel paßt.
<i>Invoke !M</i>	B-Kanäle werden zugeschaltet, wenn die Regel nicht paßt.
<i>deny M</i>	B-Kanäle werden nicht zugeschaltet, wenn die Regel paßt.
<i>deny !M</i>	B-Kanäle werden nicht zugeschaltet, wenn die Regel nicht paßt.
<i>ignore</i>	Die Regel wird ignoriert bzw. in einer Regelkette wird die Regel übersprungen.

Tabelle 8-19: **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. *aodclient*, und bestätigen Sie mit **Return**.

- 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**. Sie befinden sich wieder im Hauptmenü.

Konfigurationsbeispiele für 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 **X4000** 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**.

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*.
- 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**.

8.2.5 Layer 1 Protocol (ISDN-B-Kanal)

ISDN-B-Kanal Sie können das Layer 1 Protocol des ISDN-➤➤ **B-Kanals**, das **X4000** für Verbindungen zum WAN-Partner nutzen soll, definieren. Voreingestellt ist das Protokoll für ISDN-Datenverbindungen mit 64 kbps, was der Standard-Wert des B-Kanals ist. Ändern Sie die Einstellung nur, wenn dies ausdrücklich erforderlich ist.

Die Konfiguration erfolgt in **WAN PARTNER** ➤ **EDIT** ➤ **ADVANCED SETTINGS**:

Feld	Bedeutung
Layer 1 Protocol	Legt fest, welches Layer 1 Protocol X4000 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 8-20: **WAN PARTNER** ➤ **EDIT** ➤ **ADVANCED SETTINGS**



Für eingehende Rufe, die nicht anhand der Calling Party's Number identifiziert werden können, verwendet **X4000** als Layer 1 Protocol die Einstellungen unter **Item** in **CM-1BRI, ISDN S0** ► **INCOMING CALL ANSWERING** (siehe "[Incoming Call Answering](#)", Seite 142).

Layer 1 Protocol enthält folgende Auswahlmöglichkeiten:

Mögliche Werte	Bedeutung
<i>ISDN 64 kbps</i>	Für ISDN-Datenverbindungen mit 64 kbps. Dies ist der Standard-Wert.
<i>ISDN 56 kbps</i>	Für ISDN-Datenverbindungen mit 56 kbps.
<i>Modem</i>	(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 Modem Profile 1, die im Menü MODEM ► PROFILE CONFIGURATION ► PROFILE 1 getroffen wurden.
<i>DOVB</i>	Data transmission Over Voice Bearer – nützlich z. B. in den USA, wo Sprachverbindungen manchmal billiger sind als Datenverbindungen.
<i>V.110 (1200 ... 38400)</i>	Für GSM-Verbindungen mit V.110 mit Bit-Raten von 1200 bps, 2400 bps,..., 38400 bps.
<i>Modem Profile 1 ... 8</i>	(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 Modem Profile 1... 8, die im Menü MODEM ► PROFILE CONFIGURATION ► PROFILE 1...8 getroffen wurden.
<i>PPTP PNS</i>	Für VPN-Schnittstelle.
<i>PPP over Ethernet (PPPoE)</i>	Für Verbindungen mit ADSL (siehe Kapitel 7.2.3, Seite 157 bzw. Kapitel 9.3.2, Seite 299).

Mögliche Werte	Bedeutung
<i>AO/DI</i>	Für die Nutzung von Always On/Dynamic ISDN (AO/DI, siehe Kapitel 8.2.4, Seite 213).

Tabelle 8-21: 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 142).

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**.

8.2.6 IP Transit Network

Wenn Sie einen WAN-Partner auf **X4000** 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 **X4000** als auch für den WAN-Partner jeweils eine zusätzliche ISDN-IP-Adresse. Damit bauen Sie während der Verbindung ein virtuelles IP-Netzwerk auf, ein sog. Transitnetzwerk. Diese Einstellung benötigen Sie normalerweise nicht, nur bei manchen Spezialkonfigurationen.
- Sie weisen dem WAN-Partner dynamisch für die Dauer der Verbindung eine IP-Adresse aus einem festgelegten IP-Adreß-Pool zu.
- Sie lassen sich vom WAN-Partner dynamisch für die Dauer der Verbindung eine IP-Adresse zuweisen.

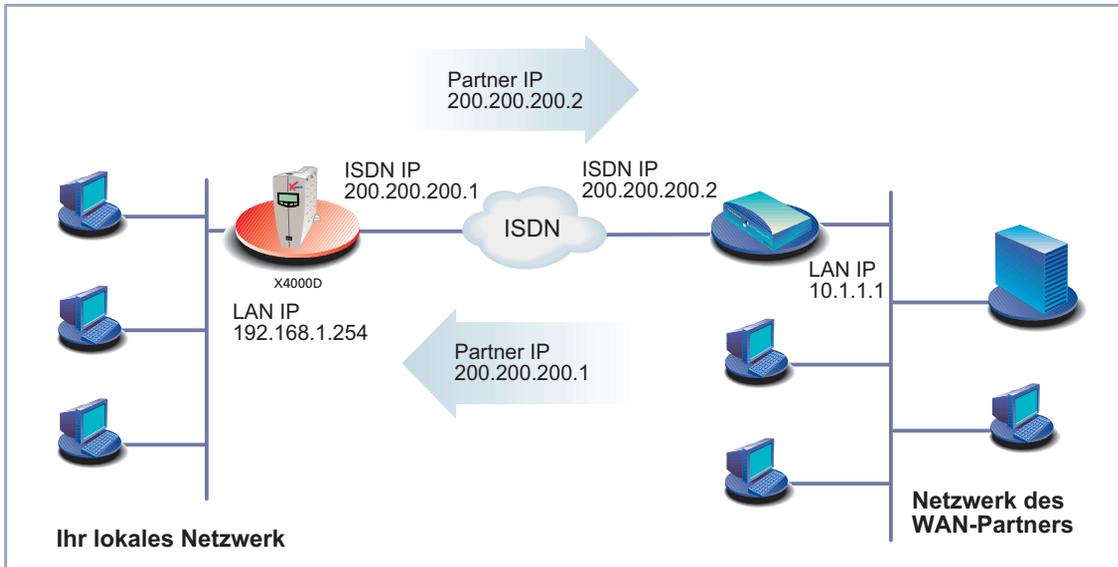


Bild 8-1: LAN-LAN-Kopplung mit Transitnetzwerk

Die Konfiguration erfolgt in **WAN PARTNER** ► **EDIT** ► **IP**:

Feld	Bedeutung
IP Transit Network	Legt fest, ob X4000 ein Transitnetzwerk zum WAN-Partner aufbaut. Mögliche Werte: siehe Tabelle 8-23, Seite 232 .
local IP Address	LAN-IP-Adresse von X4000 . Erscheint nur bei folgendem Wert für IP Transit Network : <i>no</i> . 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.
local ISDN IP Address	ISDN-IP-Adresse von X4000 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 LAN des WAN-Partners. Wenn Sie keinen Eintrag machen, trägt X4000 eine Standard-Netzmaske für die unter Partner's LAN IP Address verwendete Netzklasse ein.

Tabelle 8-22: **WAN PARTNER** ► **EDIT** ► **IP**

IP Transit Network enthält folgende Auswahlmöglichkeiten:

Mögliche Werte	Bedeutung
<i>yes</i>	Verwendung eines Transitnetzwerkes.
<i>dynamic client</i>	X4000 erhält seine IP-Adresse für die Dauer der Verbindung vom WAN-Partner.
<i>dynamic server</i>	X4000 weist dem ►► Remote-WAN-Partner für die Dauer der Verbindung eine IP-Adresse zu. Dazu muß X4000 als dynamischer IP-Adreß-Server konfiguriert sein, d. h. über einen IP-Adreß-Pool verfügen (siehe Kapitel 8.1.1, Seite 194).
<i>no</i>	Kein Transitnetzwerk. Für die meisten WAN-Partner ist diese Einstellung ausreichend.

Tabelle 8-23: **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**.

8.2.7 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 **X4000** 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 Nameservern außerhalb des LANs entstehen, niedrig gehalten und die Performanz im LAN optimiert, da Anfragen an häufig genutzte oder schon einmal aufgelöste Adressen von **X4000** selbst beantwortet werden. Die Konfiguration des DNS-Proxy finden Sie in [Kapitel 8.3.2, Seite 254](#).

Bei Eintragen eines WAN-Partners auf **X4000** können Sie festlegen, ob **X4000** Anfragen nach WINS- bzw. DNS-IP-Adressen sendet oder beantwortet.

Die Konfiguration erfolgt in:

■ **IP** ► **STATIC SETTINGS**

■ **WAN PARTNER** ► **EDIT** ► **IP** ► **ADVANCED SETTINGS**

Feld	Bedeutung
Primary Domain Name Server	IP-Adresse von X4000 s erstem globalen Domain Name Server (DNS).
Secondary Domain Name Server	IP-Adresse eines weiteren globalen Domain Name Servers.
Primary WINS	IP-Adresse von X4000 s erstem globalen WINS (Windows Internet Name Server) bzw. NBNS (NetBIOS Name Server).
Secondary WINS	IP-Adresse eines weiteren globalen WINS bzw. NBNS.

Tabelle 8-24: **IP** ► **STATIC SETTINGS**

Feld	Bedeutung
Dynamic Name Server Negotiation	Legt fest, ob X4000 IP-Adressen für Primary Domain Name Server, Secondary Domain Name Server, Primary WINS und Secondary WINS im Falle einer dynamischen Nameserver-Aushandlung vom WAN-Partner erhält oder an den WAN-Partner sendet.

Tabelle 8-25: *WAN PARTNER* ➤ *EDIT* ➤ *IP* ➤ *ADVANCED SETTINGS*

Das Feld **Dynamic Name Server Negotiation** enthält folgende Auswahlmöglichkeiten:

Mögliche Werte	Bedeutung
<i>off</i>	X4000 sendet und beantwortet keine Anfragen nach WINS- bzw. DNS-IP-Adressen.
<i>yes</i>	Das Verhalten ist an den Modus für Vergabe/Empfang einer IP-Adresse gekoppelt (Einstellung in WAN PARTNER ► EDIT ► IP unter IP Transit Network): <ul style="list-style-type: none"> ■ X4000 sendet Anfragen nach Nameserver-Adressen an den WAN-Partner, falls <i>dynamic client</i> ausgewählt ist. ■ X4000 beantwortet Anfragen des WAN-Partners nach Nameserver-Adressen vom WAN-Partner, falls <i>dynamic server</i> ausgewählt ist. ■ X4000 beantwortet, aber sendet keine Anfragen nach Nameserver-Adressen, falls <i>yes</i> oder <i>no</i> ausgewählt ist.
<i>client (receive)</i>	X4000 sendet Anfragen nach Nameserver-Adressen an den WAN-Partner.
<i>server (send)</i>	X4000 beantwortet Anfragen des WAN-Partners nach Nameserver-Adressen.

Tabelle 8-26: **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 gemacht haben (siehe [Kapitel 8.3.2, Seite 254](#)):

- 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 **X4000** die eingetragenen Nameserver-Adressen dem WAN-Partner mitteilen soll (Server-Modus) bzw. wenn bei Verbindungen zum WAN-Partner andere Nameserver-Adressen als im LAN verwendet werden sollen (Client-Modus, z. B. bei Einwahl zu einem Internet Service Provider):

- Gehen Sie zu **WAN PARTNER** ➤ **EDIT** ➤ **IP** ➤ **ADVANCED SETTINGS**.
- Wählen Sie **Dynamic Name Server Negotiation** aus.
- Bestätigen Sie mit **OK**.
- Bestätigen Sie mit **SAVE**.



Wenn Sie keinen 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.

8.2.8 Routing Information Protocol (RIP)

Routing Im Allgemeinen kann man Routing so beschreiben: Der ➤➤ **Router** empfängt ➤➤ **Datenpakete**, wobei in jedem Paket der Ziel-Host vermerkt ist. Aufgrund der Eintragungen in der sog. Routing-Tabelle (siehe "[Routing-Eintrag erstellen](#)", Seite 179) 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-Informationen zwischen mehreren Routern. Diesen Austausch regelt ein sog. Routing-Protokoll, z. B. RIP (Routing Information Protocol).

RIP Mit **➤➤ RIP** tauschen Router Ihre in Routing-Tabellen gespeicherten Informationen aus, indem sie in regelmäßigen Abständen miteinander kommunizieren und so gegenseitig Ihre Routing-Einträge ergänzen und erneuern. **X4000** 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. **X4000** kann beides.

WAN-Partner Wenn Sie mit einem WAN-Partner Empfangen und/oder Senden von RIP-Paketten vereinbaren, kann **X4000** mit den Routern im LAN des WAN-Partners dynamisch Routing-Informationen austauschen.



Der Empfang von Routing-Tabellen über RIP ist eventuell ein Sicherheitsloch, da fremde Rechner bzw. Router die Routing-Funktionalität von **X4000** verändern können.

ISDN-Verbindungen werden durch RIP-Pakete nicht aufgebaut oder gehalten.

Die Konfiguration erfolgt in:

■ **WAN PARTNER** ➤ **EDIT** ➤ **IP** ➤ **ADVANCED SETTINGS**

■ **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 8-27: **WAN PARTNER** ► **EDIT** ► **IP** ► **ADVANCED SETTINGS** bzw. **CM-100BT, FAST ETHERNET** ► **ADVANCED SETTINGS**

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

Mögliche Werte	Bedeutung
<i>none</i>	Nicht aktiviert.
<i>RIP V1</i>	Ermöglicht Senden bzw. Empfangen von RIP-Paketen der Version 1.
<i>RIP V2</i>	Ermöglicht Senden bzw. Empfangen von RIP-Paketen der Version 2.
<i>RIP V1 + V2</i>	Ermöglicht Senden bzw. Empfangen sowohl von RIP-Paketen der Version 1 als auch der Version 2.

Tabelle 8-28: **RIP Send** bzw. **RIP Receive**

ToDo Gehen Sie folgendermaßen vor:

- Gehen Sie zu **WAN PARTNER** ► **EDIT** ► **IP** ► **ADVANCED SETTINGS**.
- Wählen Sie **RIP Send** aus.
- Wählen Sie **RIP Receive** aus.
- Bestätigen Sie mit **OK**.
- Bestätigen Sie mit **SAVE**.
- Bestätigen Sie mit **SAVE**.

- Gehen Sie zu **CM-100BT, FAST ETHERNET** ➤ **ADVANCED SETTINGS**.
- Wählen Sie **RIP Send** aus.
- Wählen Sie **RIP Receive** aus.
- Bestätigen Sie mit **SAVE**.

8.2.9 Komprimierung

Datenkomprimierung Mit Hilfe von ➤➤ **Datenkomprimierung** können Sie den Datendurchsatz erhöhen und damit die Verbindungskosten senken. **X4000** unterstützt mehrere Möglichkeiten, abhängig von der gewählten ➤➤ **Enkapsulierung**, z. B. PPP (siehe [Kapitel 7.3, Seite 162](#)):

■ ➤➤ **STAC:**

Durch den in **X4000** implementierten Industriestandard STAC-Datenkomprimierung (Check Mode 3 in RFC 1974) kann der Durchsatz auf den PPP-ISDN-Verbindungen gesteigert werden.

■ MS-STAC:

STAC-Datenkomprimierung für Windows-➤➤ **Clients** (Check Mode 4 in RFC 1974). Einstellen, wenn man sich bei einem Windows Remote Access Server einwählt.

■ 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 **X4000** dies innerhalb der ➤➤ **PPP**-Verhandlungsphase und deaktiviert die Datenkomprimierung für diese Verbindung.

Die Konfiguration erfolgt in:

■ **WAN PARTNER** ➤ **EDIT**

■ **WAN PARTNER** ➤ **EDIT** ➤ **IP** ➤ **ADVANCED SETTINGS**

Feld	Bedeutung
Compression	Legt die Art der Komprimierung für Verbindungen mit dem WAN-Partner fest.

Tabelle 8-29: **WAN PARTNER** ► **EDIT**

Das Feld **Compression** enthält folgende Auswahlmöglichkeiten:

Mögliche Werte	Bedeutung
<i>none</i>	Keine Komprimierung.
<i>STAC</i>	Ermöglicht STAC-Datenkomprimierung (wenn Encapsulation = PPP).
<i>MS-STAC</i>	Ermöglicht STAC-Datenkomprimierung bei Auswahl auf einen Windows Remote Access Server (wenn Encapsulation = PPP).

Tabelle 8-30: **Compression**

Feld	Bedeutung
Van Jacobson Header Compression	Ermöglicht VJHC.

Tabelle 8-31: **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 **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**.
- Bestätigen Sie mit **SAVE**.

8.2.10 Proxy ARP (Address Resolution Protocol)

ARP-Requests Mit Hilfe von ➤➤ **Proxy ARP** kann **X4000** ➤➤ **ARP-Requests** aus dem LAN beantworten. Wenn ein Host im LAN zu einem anderen Host im LAN oder zu einem WAN-Partner eine Verbindung aufbauen will, aber dessen Hardware-Adresse nicht kennt, sendet er einen sog. ARP-Request als ➤➤ **Broadcast** ins Netz. Er stellt also eine Frage an alle: "Wie lautet die Hardware-Adresse von Host x?". Wenn auf **X4000** Proxy ARP aktiviert ist und der gewünschte Host über eine definierte WAN-Verbindung erreichbar ist, beantwortet **X4000** den ARP-Request mit seiner eigenen Hardware-Adresse. Dies ist für den Verbindungsaufbau ausreichend: Die ➤➤ **Datenpakete** werden an **X4000** geschickt, der sie dann an den gewünschten Host weiterleitet.

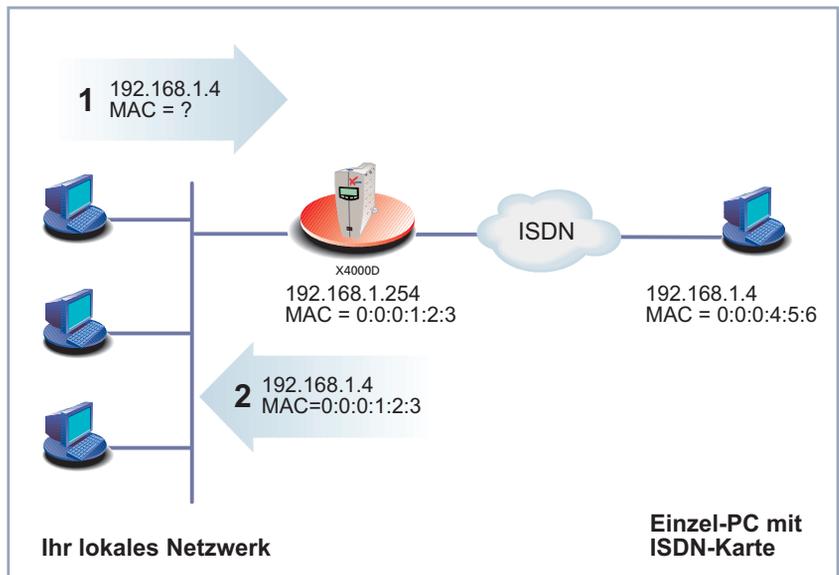


Bild 8-2: Proxy ARP

Die Konfiguration erfolgt in:

■ **WAN PARTNER** ➤ **EDIT** ➤ **IP** ➤ **ADVANCED SETTINGS**

■ **CM-100BT, FAST ETHERNET** ➤ **ADVANCED SETTINGS**

Feld	Bedeutung
Proxy Arp	Ermöglicht X4000 , ARP-Requests zu beantworten.

Tabelle 8-32: **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
<i>off</i>	Deaktiviert Proxy ARP über die Schnittstelle zum WAN-Partner.
<i>on (up or dormant)</i>	X4000 beantwortet einen ARP-Request nur, wenn der Status der Verbindung zum WAN-Partner <i>up</i> (aktiv) oder <i>dormant</i> (ruhend) ist. Bei <i>dormant</i> beantwortet X4000 lediglich den ARP-Request, der Verbindungsaufbau erfolgt erst, wenn jemand tatsächlich die Route nutzen will.
<i>on (up only)</i>	X4000 beantwortet einen ARP-Request nur, wenn der Status der Verbindung zum WAN-Partner <i>up</i> (aktiv) ist, wenn also bereits eine Verbindung zum WAN-Partner besteht.

Tabelle 8-33: **Proxy Arp**

Proxy Arp in **CM-100BT, FAST ETHERNET** ► **ADVANCED SETTINGS** enthält folgende Auswahlmöglichkeiten:

Mögliche Werte	Bedeutung
<i>off</i>	Deaktiviert Proxy ARP über die LAN-Schnittstelle.
<i>on</i>	Ermöglicht Proxy ARP über die LAN-Schnittstelle.

Tabelle 8-34: **Proxy Arp**

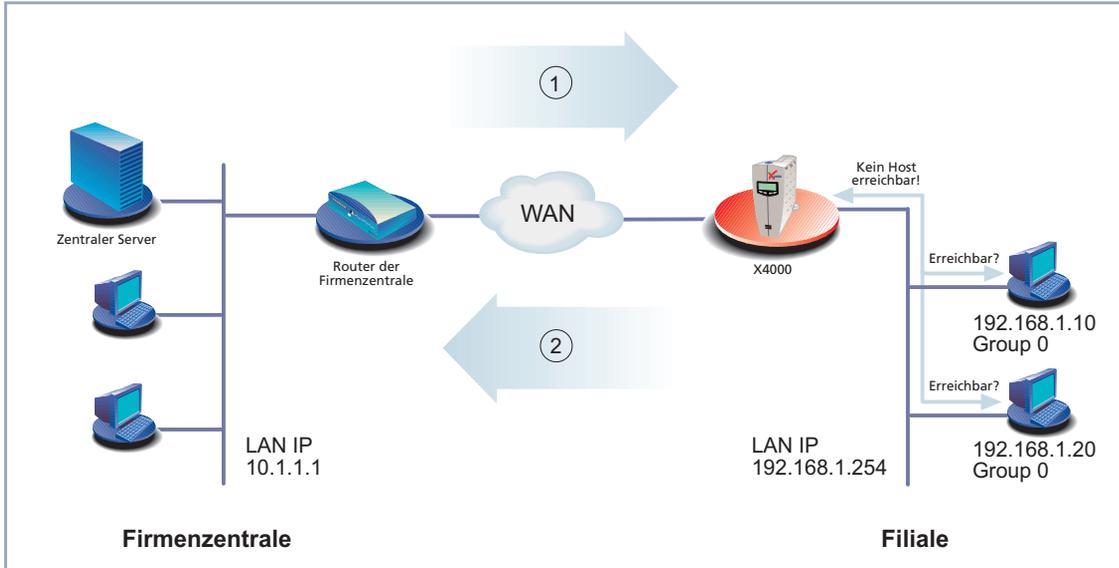
ToDo Gehen Sie folgendermaßen vor:

- Gehen Sie zu **WAN PARTNER** ► **EDIT** ► **IP** ► **ADVANCED SETTINGS**.
- Wählen Sie **Proxy Arp** aus.
- Bestätigen Sie mit **SAVE**.
- Bestätigen Sie mit **SAVE**.
- Gehen Sie zu **CM-100BT, FAST ETHERNET** ► **ADVANCED SETTINGS**.
- Wählen Sie **Proxy Arp** aus.
- Bestätigen Sie mit **SAVE**.
- Bestätigen Sie mit **SAVE**.

8.2.11 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 8-3, Seite 244](#)), befindet sich häufig ein zentraler Server im LAN der Firmenzentrale. Wenn dieser zentrale Server so konfiguriert ist, daß er regelmäßig WAN-Verbindungen zu **X4000** 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.



1	Versuch eines Verbindungsaufbaus	2	X4000 ist "besetzt", keine Verbindung möglich
---	----------------------------------	---	--

Bild 8-3: Keepalive Monitoring

Kosten senken Mit der Funktion Keepalive Monitoring können Sie **X4000** in der Filiale so konfigurieren, daß unnötige WAN-Verbindungen von der Firmenzentrale zur Filiale vermieden werden. In regelmäßigen, einstellbaren Abständen überprüft **X4000**, 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 ein Verbindungsaufbau durch den zentralen Server verhindert, indem **X4000** die Schnittstelle zum WAN-Partner "Firmenzentrale" deaktiviert. Als Resultat scheint die Leitung zur Filiale besetzt zu sein, wenn der zentrale Server der Firmenzentrale eine Verbindung aufzubauen versucht. 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 **X4000** 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 **X4000** die erneute Erreichbarkeit signalisiert, ist abhängig vom eingestellten Überwachungsintervall (**Interval**).



Der entsprechende WAN-Partner, also z. B. die Firmenzentrale, sollte auf **X4000** per CLID (Calling Line Identification) identifiziert werden können. Wenn dies nicht der Fall ist, kann Keepalive Monitoring u. U. unwirksam sein.



Wenn Keepalive Monitoring auf **X4000** für WAN-Partner eingerichtet wird, die über einen RADIUS-Server authentisiert werden, funktioniert Keepalive Monitoring nicht. Die entsprechenden unnötigen Verbindungen können auf diese Weise also nicht verhindert werden!

Die Konfiguration erfolgt in **SYSTEM** ► **KEEPLIVE MONITORING** ► **ADD**:

Feld	Bedeutung
Group	<p>Definiert eine Gruppe von Hosts, deren Erreichbarkeit von X4000 überwacht werden soll. Jeder zu überwachende Host wird einer Gruppe zugeordnet. Insgesamt können zehn Gruppen mit jeweils bis zu zehn Hosts angelegt werden.</p> <p>Mögliche Werte: 0 ... 9</p>
IPAddress	<p>Definiert einen Host, der von X4000 überwacht werden soll.</p>
Interval	<p>Definiert ein Zeitintervall in s, welches zur Überprüfung der Erreichbarkeit von Hosts verwendet werden soll (Standardwert: 300).</p> <p>Innerhalb einer Gruppe wird das kleinste Zeitintervall verwendet. D. h. alle Hosts einer Gruppe werden von X4000 im dem Zeitintervall überprüft, das den kleinsten Wert in der Gruppe darstellt.</p>
DownAction	<p>Definiert, wie der Status der unter FirstIfIndex und Range festgelegten X4000-Schnittstellen gesetzt wird, wenn ALLE Hosts einer Gruppe nicht erreichbar sind. Mögliche Werte:</p> <ul style="list-style-type: none"> ■ <i>down</i> (Standardwert): Schnittstellen werden deaktiviert. ■ <i>up</i>: Schnittstellen werden aktiviert. <p>Wenn mindestens ein Host einer Gruppe wieder erreichbar ist, wird der Status der Schnittstellen wieder auf den ursprünglichen Wert gesetzt.</p>

Feld	Bedeutung
FirstfIndex	<p>Definiert die erste Schnittstelle eines Schnittstellen-Bereiches auf X4000, für die die unter DownAction festgelegte Aktion ausgeführt werden soll.</p> <p>Mögliche Werte: 10001 ... 15000 (Standardwert: 10001).</p> <p>Für Wählverbindungen zu WAN-Partnern sind Schnittstellen mit Indizes von 10001 bis 15000 vorgesehen. Der Standardwert 10001 bezeichnet die Schnittstelle zum ersten auf X4000 konfigurierten WAN-Partner (Wählverbindung). Die Indizes anderer Schnittstellen finden Sie in der Software Reference.</p>
Range	<p>Definiert den Bereich von Schnittstellen auf X4000, für die die unter DownAction festgelegte Aktion ausgeführt werden soll.</p> <p>Wenn Sie FirstfIndex = 10001 und Range = 0 einstellen, ist nur die Schnittstelle mit dem Index 10001 betroffen.</p> <p>Wenn Sie FirstfIndex = 10001 und Range = 4999 (Standardwert) einstellen, sind die Schnittstellen mit den Indizes 10001 bis 15000 betroffen.</p>

Tabelle 8-35: **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 8-3, Seite 244](#) dargestellte Beispiel zu konfigurieren:

► Gehen Sie zu **SYSTEM** ► **KEEPALIVE MONITORING**.

- Drücken Sie **ADD**, um den ersten Host hinzuzufügen, der mit Keepalived Monitoring von **X4000** 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 **FirstIndex** ein: **1001**.
- Geben Sie **Range** ein: **4999**.
- Bestätigen Sie mit **SAVE**.
- Drücken Sie **ADD**, um den zweiten Host hinzuzufügen.
- 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 **FirstIndex** ein: **1001**.
- Geben Sie **Range** ein: **4999**.
- Bestätigen Sie mit **SAVE**.

Mit diesen Einstellungen erreichen Sie, daß **X4000** in Abständen von 300 s 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 **X4000** für Wählverbindungen zu WAN-Partnern deaktiviert. Die Überprüfung der Hosts durch **X4000** geht mit dem Zeitintervall 300 s weiter und sobald mindestens einer wieder erreichbar ist, aktiviert **X4000** die Schnittstellen wieder.

8.3 Grundlegende IP-Einstellungen

Hier finden Sie einige grundlegende Einstellungen, die Sie auf **X4000** festlegen können:

- Beziehen der Systemzeit ([Kapitel 8.3.1, Seite 249](#))
- Namensauflösung (➤➤ **DNS**) auf **X4000** ([Kapitel 8.3.2, Seite 254](#))
- ➤➤ **Port**-Nummern ([Kapitel 8.3.3, Seite 274](#))
- ➤➤ **BOOTP** Relay Agent ([Kapitel 8.3.4, Seite 275](#))

Im folgenden werden die jeweils erforderlichen Konfigurationsschritte erläutert.

8.3.1 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 250).
- manuell auf **X4000** einstellen (siehe "[Systemzeit manuell einstellen](#)", Seite 253).

Systemzeit automatisch beziehen

Die Konfiguration erfolgt in **IP** ► **STATIC SETTINGS**.

Feld	Bedeutung
Time Protocol	<p>Protokoll, das für das Beziehen der aktuellen Zeit benutzt wird. Mögliche Werte:</p> <ul style="list-style-type: none"> ■ <i>TIME/UDP</i> ■ <i>TIME/TCP</i> ■ <i>SNTP</i> ■ <i>ISDN</i> ■ <i>none</i>
Time Offset (sec)	<p>Anzahl der Sekunden, die zu der bezogenen Zeit addiert oder subtrahiert wird. Wenn Sie Werte zwischen -24 und +24 eingeben, versteht X4000 die Angabe als Anzahl von Stunden und wandelt sie nach dem Drücken von SAVE automatisch in die entsprechende Anzahl von Sekunden um. Beachten Sie: Wenn Sie <i>ISDN</i> als Time Protocol wählen, müssen Sie den Time Offset auf 0 setzen.</p> <p>Wenn Sie Time Offset (sec) verändern (Zeit zurückstellen), sollte kein Datenfluß bestehen.</p>

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 X4000 die Angabe als Anzahl von Stunden und wandelt sie nach dem Drücken 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 X4000 nutzt. Time Server wird nicht benötigt, wenn Sie ISDN als Time Protocol einstellen.

Tabelle 8-36: **IP »» STATIC SETTINGS**

Das Feld **Time Protocol** enthält folgende Auswahlmöglichkeiten:

Mögliche Werte	Bedeutung
<i>TIME/UDP</i>	Systemzeit (RFC 868) über »» UDP .
<i>TIME/TCP</i>	Systemzeit (RFC 868) über »» TCP .
<i>TIME/SNTP</i>	Systemzeit per SNTP (Simple Network Time Protocol, RFC 1769) über UDP.
<i>ISDN</i>	Systemzeit aus ISDN- »» D-Kanal (kostenlos).
<i>none</i>	Keine Systemzeit beziehen.

Tabelle 8-37: **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**.
Nachdem die erste ISDN-Verbindung beendet wurde, bezieht **X4000** die Systemzeit über ISDN.

Time-Server Gehen Sie folgendermaßen vor, um die Systemzeit von einem Time-Server zu beziehen:

- Gehen Sie zu **IP** ➤ **STATIC SETTINGS**.
- Wählen Sie **Time Protocol** aus, z. B. *TIME/UDP*.
- Geben Sie **Time Offset (sec)** ein, z. B. *0*.
- Geben Sie **Time Update Interval (sec)** ein, z. B. *86400* (entspricht 24 Stunden).
- Geben Sie IP-Adresse oder Hostname für **Time Server** ein.
- Bestätigen Sie mit **SAVE**.

X4000 bezieht somit die Systemzeit über einen Time-Server. Alle 24 Stunden gleicht **X4000** 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 **X4000** der Time-Server der **DIME Tools** auf Ihrem PC aktiv ist.



Wenn Ihr Rechner keine feste IP-Adresse hat, sondern seine IP-Adresse via ➤➤ **DHCP** dynamisch zugewiesen bekommt, können Sie Ihren Rechner nicht als Time-Server verwenden.

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 X4000 eingestellte Systemzeit an (Datum und Uhrzeit).
New Time:	Hier wird die neue Uhrzeit eingegeben, die X4000 verwenden soll (Stunden:Minuten).
New Date:	Hier wird das neue Datum eingegeben, das X4000 verwenden soll (Monat/Tag/Jahr).

Tabelle 8-38: **SYSTEM** ➤ **TIME AND DATE**

Gehen Sie folgendermaßen vor, um die Systemzeit auf **X4000** manuell einzugeben:



Wenn auf **X4000** zusätzlich eine Methode zum automatischen Beziehen der Zeit festgelegt ist, haben die auf diese Weise erhaltenen Werte höhere Priorität. D. h. falls **X4000** ein entsprechendes Zeit-Signal 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 **X4000** neu eingestellte Systemzeit angezeigt.

8.3.2 Namensauflösung - X4000 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 anpingen möchten 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 Hostnamen 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 Nameserver an die Quelle der Anfrage geschickt. Nameserver bilden eine hierarchische Baumstruktur. Wenn also ein Nameserver einen Namen nicht auflösen kann, fragt er bei einem übergeordneten Nameserver nach usw.

■ **HOSTS-Dateien:**

Auf HOSTS-Dateien, die sich auf den PCs im LAN befinden, legen Sie eine Tabelle von Hostnamen 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 X4000

X4000 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 via Setup Tool, um einen Überblick über DNS-Anfragen auf **X4000** zu ermöglichen.

So funktioniert's im Einzelnen:

DNS-Proxy Der DNS-Proxy macht das umständliche Pflegen von HOSTS-Dateien auf Rechnern im LAN überflüssig, da Sie **X4000** als DNS-Server auf den entsprechenden Rechnern eintragen können. DNS-Anfragen werden vom Rechner an **X4000** 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-Server-Einträge haben, sondern diese dynamisch von **X4000** als DHCP-Server zugewiesen bekommen.

Durch Forwarding-Einträge kann **X4000** entscheiden, welcher DNS-Server zur Auflösung bestimmter Namen herangezogen werden soll. Wenn Sie also z. B. auf **X4000** 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 **X4000** an einen DNS-Server weitergeleitet und von diesem mit einem DNS-Record beantwortet wird, wird der so aufgelöste Name mit der zugehörigen IP-Adresse als positiver dynamischer Eintrag im DNS-Cache auf **X4000** gespeichert. Wenn also ein einmal aufgelöster Name erneut benötigt wird, kann **X4000** die Anfrage aus dem Cache beantworten, eine Anfrage an einen externen Nameserver 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 Ablauf der TTL wird ein dynamischer Eintrag aus dem Cache gelöscht.

Statische Namenseinträge

Mit positiven statischen Einträgen geben Sie auf **X4000** Namen mit den dazugehörigen IP-Adressen ein. Wenn Sie auf diese Weise häufig benötigte IP-Adressen speichern, kann **X4000** entsprechende DNS-Anfragen selbst beantworten, die Verbindung zu einem externen Nameserver ist nicht nötig. Damit wird der Zugriff auf diese Adressen beschleunigt. Für ein kleines Netzwerk kann so ein Nameserver auf **X4000** 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 Nameserver weitergeleitet.



Einen dynamischen Eintrag können Sie in **IP** ➔ **DNS** ➔ **DYNAMIC CACHE** ganz einfach per "Knopfdruck" in einen statischen umwandeln (siehe [Tabelle 8-43, Seite 267](#)).

Filterfunktion

Durch Verwendung von negativen statischen Einträgen können Sie die Namensauflösung auf **X4000** 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 **X4000** 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 **X4000** oder durch einen anderen Nameserver aufgelöst wird (siehe [Kapitel 14.1, Seite 428](#)). Hilfe zu dem Kommando erhalten Sie durch Eingabe von `nslookup -?`.

Weitere Möglichkeiten

Globale Nameserver Desweiteren können Sie unter **IP** ► **STATIC SETTINGS** die IP-Adresse von globalen Nameservern eintragen, die bevorzugt befragt werden sollen, wenn **X4000** Anfragen nicht selbst oder durch Forwarding-Einträge beantworten kann.

Für lokale Anwendungen kann als globaler Nameserver die IP-Adresse von **X4000** oder die Loopback-Adresse (127.0.0.1) eingetragen werden.

Die Adressen von Nameservern kann **X4000** gegebenenfalls an WAN-Partner übermitteln bzw. von WAN-Partnern erhalten:

Default Interface Zudem können Sie unter **Default Interface** einen WAN-Partner auswählen, zu dem standardmäßig für eine Nameserver-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 **X4000** als DHCP-Server konfiguriert ist, können den DHCP-Clients im LAN IP-Adressen von Nameservern übermittelt werden. Dabei können die Adressen der auf **X4000** eingetragenen globalen Nameserver übermittelt werden oder die Adresse von **X4000** selbst. Im letzteren Fall gehen DNS-Anfragen

von den DHCP-Clients an **X4000**, der diese entweder selbst beantwortet oder gegebenenfalls weiterleitet (Proxy-Funktion).

Austausch von DNS-Server-Adressen mit WAN-Partnern

IPCP Das gleiche gilt, wenn bei der IP-Konfiguration eines WAN-Partners die dynamische Aushandlung von Nameservern aktiviert ist und **X4000** im Server-Modus arbeitet (**Dynamic Name Server Negotiation = server (send)**). In diesem Fall können bei Nameserver-Verhandlungen über IPCP mit dem WAN-Partner, der IP-Adress-Client ist, ebenfalls die Adressen der globalen Nameserver oder die Adresse von **X4000** selbst übermittelt werden.

Wenn **X4000** im Client-Modus arbeitet (**Dynamic Name Server Negotiation = client (receive)**), können gegebenenfalls Nameserver-Adressen mit dem WAN-Partner, der IP-Adress-Server ist, ausgehandelt und an **X4000** übermittelt werden. Diese können als globale Nameserver auf **X4000** eingetragen werden und somit für zukünftige Namensauflösungen zur Verfügung stehen.

Strategie zur Namensauflösung auf X4000

Eine DNS-Anfrage wird von **X4000** 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 Nameserver eingetragen?
In diesem Fall werden die entsprechenden DNS-Server befragt. Ist für lokale Anwendungen die IP-Adresse von **X4000** 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 Nameserver 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 Nameserver 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 Nameserver-Aushandlung werden diese als globale Nameserver eingetragen und stehen somit für weitere Anfragen zur Verfügung.
6. Anfrage wird mit Server-Fehler 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 **X4000** erfolgt in:

- **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**
- IP ► STATIC SETTINGS** enthält folgende Felder:

Feld	Bedeutung
Domain Name	Legt X4000s Domain Name fest.
Primary Domain Name Server	IP-Adresse von X4000s erstem globalen Domain Name Server (DNS).
Secondary Domain Name Server	IP-Adresse eines weiteren globalen Domain Name Servers.
Primary WINS	IP-Adresse von X4000s erstem globalen WINS (Windows Internet Name Server) bzw. NBNS (NetBIOS Name Server).
Secondary WINS	IP-Adresse eines weiteren globalen WINS bzw. NBNS.

Tabelle 8-39: **IP ► STATIC SETTINGS**

IP ► DNS enthält folgende Felder:

Feld	Bedeutung
Positive Cache	<p>Ermöglicht positive dynamische Einträge im Cache. Mögliche Werte:</p> <ul style="list-style-type: none">■ <i>enabled</i> (Standardwert): Erfolgreich aufgelöste Namen und IP-Adressen werden im Cache gespeichert.■ <i>flush</i>: Alle positiven dynamischen Einträge im Cache werden gelöscht.■ <i>disabled</i>: 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	<p>Ermöglicht negative dynamische Einträge im Cache. Mögliche Werte:</p> <ul style="list-style-type: none">■ <i>enabled</i> (Standardwert): Namen, die nicht aufgelöst werden konnten, werden als negative Einträge im Cache gespeichert.■ <i>flush</i>: Alle negativen dynamischen Einträge im Cache werden gelöscht.■ <i>disabled</i>: 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	<p>Legt fest, ob die Adressen von globalen Nameservern auf X4000 (in IP ► STATIC SETTINGS) mit von WAN-Partnern übermittelten Nameserver-Adressen überschrieben werden dürfen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ■ <i>yes</i> (Standardwert) ■ <i>no</i>
Default Interface	<p>Legt den WAN-Partner fest, zu dem standardmäßig eine Verbindung zur Nameserververhandlung aufgebaut wird, wenn andere Versuche zur Namensauflösung nicht erfolgreich waren.</p>
DHCP Assignment	<p>Legt fest, welche Nameserver-Adressen dem DHCP-Client übermittelt werden, wenn X4000 als DHCP-Server konfiguriert ist. Mögliche Werte:</p> <ul style="list-style-type: none"> ■ <i>none</i>: Es wird keine Nameserver-Adresse übermittelt. ■ <i>self</i> (Standardwert): Es wird die Adresse von X4000 als Nameserver-Adresse übermittelt. ■ <i>global</i>: Es werden die Adressen der auf X4000 eingetragenen globalen Nameserver übermittelt.

Feld	Bedeutung
IPCP Assignment	<p>Legt fest, welche Nameserver-Adressen von X4000 bei einer dynamischen Nameserver-Verhandlung an einen WAN-Partner übermittelt werden. Mögliche Werte:</p> <ul style="list-style-type: none">■ <i>none</i>: Es wird keine Nameserver-Adresse übermittelt.■ <i>self</i>: Es wird die Adresse von X4000 als Nameserver-Adresse übermittelt.■ <i>global</i> (Standardwert): Es werden die Adressen der auf X4000 eingetragenen globalen Nameserver 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 8-40: **IP** ➔ **DNS**

IP ➤ **DNS** ➤ **STATIC Hosts** ➤ **ADD** enthält folgende Felder:

Feld	Bedeutung
Default Domain:	Der in IP ➤ STATIC SETTINGS eingetragene Domain Name von X4000 wird angezeigt.
Name	<p>Hostname, dem Address mit diesem statischen Eintrag zugeordnet wird. Kann auch Wildcards (*) enthalten (nur am Anfang von Name, z. B. *.bintec.de).</p> <p>Bei Eingabe eines unvollständigen Namens ohne Punkt wird dieser nach Bestätigung mit SAVE mit "Default Domain" vervollständigt.</p>
Response	<p>Legt fest, welcher Art der statische Eintrag ist. Mögliche Werte:</p> <ul style="list-style-type: none"> ■ <i>positive</i> (Standardwert): Ein DNS-Request nach Name wird mit einem DNS-Record beantwortet, der die dazugehörige Address enthält. ■ <i>ignore</i>: Ein DNS-Request wird ignoriert, es wird keine Antwort gegeben (auch keine negative). ■ <i>negative</i>: Ein DNS-Request nach Name wird mit einer negativen Antwort beantwortet.
Address	<p>(nur bei Response = <i>positive</i>) IP-Adresse, die Name zugeordnet wird.</p>
TTL	<p>Gültigkeitsdauer der Zuordnung von Name zu Address in s (nur relevant bei Response = <i>positive</i>). Dieser Wert wird dem TTL-Feld (Time To Live) gegeben, falls X4000 einen entsprechenden DNS-Record verschickt.</p> <p>Standardwert: <i>86400</i> (= 24 h)</p>

Tabelle 8-41: **IP** ➤ **DNS** ➤ **STATIC Hosts** ➤ **ADD**

IP ➤ **DNS** ➤ **FORWARDED DOMAINS** ➤ **ADD** enthält folgende Felder:

Feld	Bedeutung
Global Nameservers:	Die in IP ➤ STATIC SETTINGS eingetragenen globalen Nameserver werden angezeigt.
Default Domain:	Der in IP ➤ STATIC SETTINGS eingetragene Domain Name von X4000 wird angezeigt.
Name	<p>Hostname, der mit diesem Forwarding-Eintrag aufgelöst werden soll. Kann auch Wildcards enthalten (nur am Anfang von Name, z. B. *.bintec.de).</p> <p>Bei Eingabe eines unvollständigen Namens ohne Punkt wird dieser nach Bestätigung mit SAVE mit ".Default Domain" vervollständigt.</p>
Interface	Legt den WAN-Partner fest, zu dem zur Auflösung von Name eine Verbindung aufgebaut wird.
TTL	<p>Gültigkeitsdauer der Zuordnung von Name zu Address in s.</p> <p>Standardwert: 86400 (= 24 h)</p> <p>Wenn die Anfrage von X4000 nach Name mit einem DNS-Record beantwortet wird, enthält dieser ein TTL-Feld (= Time To Live in s), dessen Wert bei Weiterleiten des DNS-Records von X4000 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.</p>

Tabelle 8-42: **IP** ➤ **DNS** ➤ **FORWARDED DOMAINS** ➤ **ADD**

IP ➤ **DNS** ➤ **DYNAMIC CACHE** enthält folgende Felder:

Feld	Bedeutung
Name	Hostname, dem Address mit diesem dynamischen Eintrag im Cache zugeordnet wird.
Address	IP-Adresse, die Name zugeordnet wird.
Resp	<p>Legt fest, welcher Art der dynamische Eintrag ist. Mögliche Werte:</p> <ul style="list-style-type: none"> ■ <i>positive</i>: Ein DNS-Request nach Name wird aus dem Cache mit der dazugehörigen IP-Adresse beantwortet. ■ <i>negative</i>: Ein DNS-Request nach Name wird aus dem Cache mit einer negativen Antwort beantwortet.
TTL	<p>Gibt an, wie viele Sekunden der dynamische Eintrag noch im Cache bleibt. Nach Ablauf von TTL wird der Eintrag gelöscht.</p> <p>Bei Speicherung eines positiven dynamischen Eintrags im Cache wird hier der Wert des im DNS-Record enthaltenen TTL-Felds (= Time To Live in s) 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.</p> <p>Bei Speicherung eines negativen dynamischen Eintrags im Cache wird hier immer Maximum TTL for Neg Cache entries vergeben.</p>
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 8-43: **IP ➤ DNS ➤ DYNAMIC CACHE**

IP ➤ **DNS** ➤ **ADVANCED SETTINGS...** enthält folgende Felder:

Feld	Bedeutung
Maximum Number of DNS Records	<p>Legt die maximale Anzahl der statischen und dynamischen Einträge fest.</p> <p>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.</p> <p>Wird Maximum Number of DNS Records vom Benutzer heruntersgesetzt, werden gegebenenfalls dynamische Einträge gelöscht.</p> <p>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!</p>
Maximum TTL for Pos Cache entries	<p>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.</p>
Maximum TTL for Neg Cache Entries	<p>Wird einem negativen dynamischen Eintrag im Cache als TTL vergeben.</p>

Tabelle 8-44: **IP** ➤ **DNS** ➤ **ADVANCED SETTINGS...**

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 Nameserver weitergeleitet wurden.
Cache Hitrate (%)	Zeigt die Anzahl von Cache Hits pro DNS Requests in % 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 Nameserver (weder positiv noch negativ) beantworten konnte.

Tabelle 8-45: **IP** ► **DNS** ► **GLOBALS STATISTICS...**

Folgender Teil von **WAN PARTNER** ➤ **EDIT** ➤ **IP** ➤ **ADVANCED SETTINGS** ist für diesen Konfigurationsschritt interessant:

Feld	Bedeutung
Dynamic Name Server Negotiation	Legt fest, ob X4000 IP-Adressen für Primary Domain Name Server , Secondary Domain Name Server , Primary WINS und Secondary WINS im Falle einer dynamischen Nameserver-Aushandlung vom WAN-Partner erhält oder an den WAN-Partner sendet.

Tabelle 8-46: **WAN PARTNER** ➤ **EDIT** ➤ **IP** ➤ **ADVANCED SETTINGS**

Das Feld **Dynamic Name Server Negotiation** enthält folgende Auswahlmöglichkeiten:

Mögliche Werte	Bedeutung
<i>off</i>	X4000 sendet und beantwortet keine Anfragen nach Nameserver-Adressen.
<i>yes</i>	Das Verhalten ist an den Modus für Vergabe/Empfang einer IP-Adresse gekoppelt (Einstellung in WAN PARTNER ► EDIT ► IP unter IP Transit Network): <ul style="list-style-type: none"> ■ X4000 sendet Anfragen nach Nameserver-Adressen an den WAN-Partner, falls <i>dynamic client</i> ausgewählt ist. ■ X4000 beantwortet Anfragen des WAN-Partners nach Nameserver-Adressen vom WAN-Partner, falls <i>dynamic server</i> ausgewählt ist. ■ X4000 beantwortet, aber sendet keine Anfragen nach Nameserver-Adressen, falls <i>yes</i> oder <i>no</i> ausgewählt ist.
<i>client (receive)</i>	X4000 sendet Anfragen nach Nameserver-Adressen an den WAN-Partner.
<i>server (send)</i>	X4000 beantwortet Anfragen des WAN-Partners nach Nameserver-Adressen.

Tabelle 8-47: **Dynamic Name Server Negotiation**

Konfiguration mit dem Setup Tool – Vorgehensweise

ToDo Gehen Sie folgendermaßen vor, um Namensauflösung mit dem DNS-Proxy auf **X4000** zu konfigurieren:

Namensauflösung auf X4000 Tragen Sie gegebenenfalls zunächst globale Nameserver auf **X4000** 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 Nameserver 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** machen 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**.

X4000 ↔ WAN-Partner

Wenn Sie einen WAN-Partner so konfigurieren möchten, daß die Adresse eines Nameservers gegebenenfalls von **X4000** an den WAN-Partner oder vom WAN-Partner an **X4000** übermittelt wird, gehen Sie folgendermaßen vor:

- Gehen Sie zu **WAN PARTNER** ➤ **EDIT** ➤ **IP** ➤ **ADVANCED SETTINGS**.
- Wählen Sie **Dynamic Name Server Negotiation** aus.
- Bestätigen Sie mit **OK**.
- Bestätigen Sie mit **SAVE**.

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.

8.3.3 Portnummern

Was ist ein ➤➤ Port? **X4000** verfügt über mehrere Dienste bzw. Applikationen, z. B. HTTP, ➤➤ **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 **X4000** neben der IP-Adresse auch einen Port an. So wird die entsprechende Applikation angesprochen. Ports gibt es nur bei den Protokollen TCP und UDP!

X4000 leitet eingehende ➤➤ **Datenpakete** an den Port mit der zur gewünschten Applikation gehörigen Nummer weiter. Damit wird die entsprechende Applikation von **X4000** angesprochen, die eingehenden Daten können verarbeitet werden.

In **IP** ➤ **STATIC SETTINGS** können Sie einige wichtige Portnummern festlegen:



Normalerweise sind die Einstellungen korrekt. Nehmen Sie hier also nur Änderungen vor, wenn dies nötig ist.

Feld	Bedeutung
Remote CAPI Server TCP port	Port-Nummer für ►► Remote-CAPI -Verbindungen: 2662 (festgelegt von IANA, www.iana.com).
Remote TRACE Server TCP port	Port-Nummer für TRACE-Requests. Standardwert: 7000.
RIP UDP port	Port-Nummer für ►► RIP (Routing Information Protocol). Standardwert: 520. Mit RIP UDP port = 0 kann RIP ausgeschaltet werden.
HTTP TCP port	Port-Nummer für HTTP-Requests. Standardwert: 80. Mit HTTP TCP port = 0 wird der Zugriff auf die HTTP-Statusseite von X4000 (siehe Kapitel 10.1.4, Seite 332) verhindert.

Tabelle 8-48: **IP** ► **STATIC SETTINGS**

ToDo Gehen Sie folgendermaßen vor, wenn Sie eine der Portnummern verändern wollen:

- Gehen sie zu **IP** ► **STATIC SETTINGS**.
- Geben Sie **Remote CAPI Server TCP port**, **Remote TRACE Server TCP port**, **RIP UDP port** und/oder **HTTP TCP port** ein.
- Bestätigen Sie mit **SAVE**.

8.3.4 BOOTP Relay Agent

Bootstrap Protocol Das Bootstrap Protocol (►► **BOOTP**) definiert, wie ein Host (**BOOTP-Client**) in einem TCP/IP-Netzwerk beim Hochfahren seine IP-Adresse und andere Konfigurationsinformationen erhält. Der **BOOTP-Client** sendet einen **BOOTP-Request**, ein **BOOTP-Server** beantwortet den Request mit einem **BOOTP-Response** und versorgt den Client mit den erforderlichen Informationen. Da der Server nur Requests aus dem LAN, in dem er sich befindet, hört, ist das Einrichten eines **BOOTP-Relay-Agent** manchmal sinnvoll. Der Agent lei-

tet alle Requests bzw. Responses zwischen Client und Server über eine WAN-Verbindung zu diesem Server weiter.

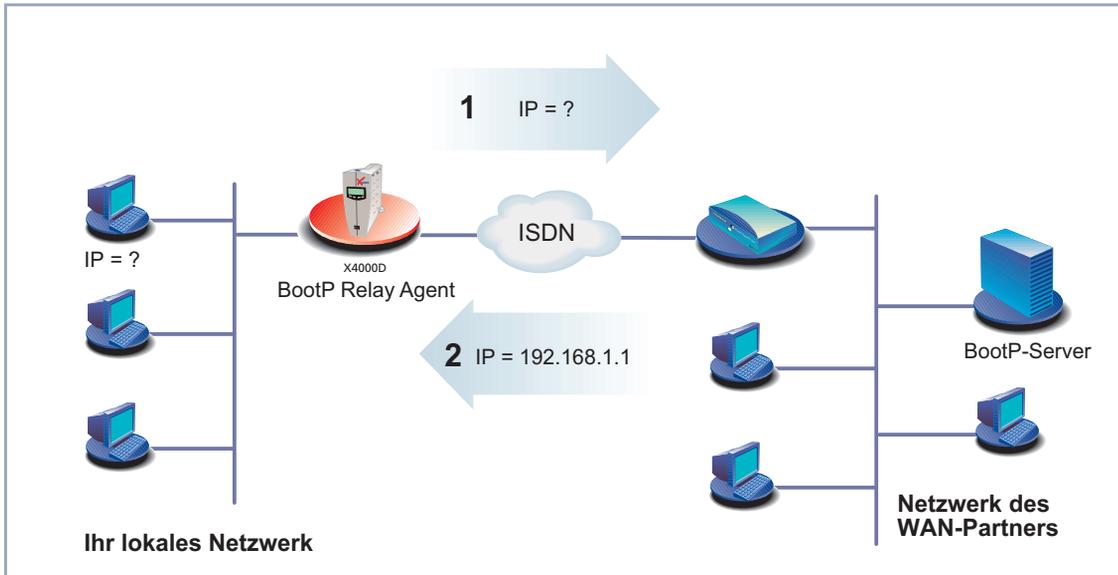


Bild 8-4: X4000 als BOOTP-Relay-Agent

Die Konfiguration erfolgt in **IP** ► **STATIC SETTINGS**:

Feld	Bedeutung
BOOTP Relay Server	IP-Adresse des BOOTP-Servers.

Tabelle 8-49: **IP** ► **STATIC SETTINGS**

ToDo Gehen Sie folgendermaßen vor:

- Gehen Sie zu **IP** ► **STATIC SETTINGS**.
- Geben Sie **BOOTP Relay Server** ein.
- Bestätigen Sie mit **SAVE**.



Wenn für die Verbindung zwischen BOOTP-Server und BOOTP-Client eine WAN-Verbindung erforderlich ist, muß ein entsprechender WAN-Partner eingerichtet sein (siehe [Kapitel 7.3, Seite 162](#)).

8.4 IPX-Einstellungen

➤➤ **IPX**-Protokoll (Internet Packet Exchange Protocol) ist ein Netzwerkprotokoll, das hauptsächlich in Novell-Netzwerken verwendet wird. Mit Hilfe von IPX können Novell-➤➤ **Clients** und Novell-➤➤ **Server** über LAN/WAN-Verbindungen kommunizieren.

Im folgenden werden die Konfigurationsschritte erläutert, die für IPX-Verbindungen erforderlich sind:

- Allgemeine Einstellungen
- LAN-Schnittstelle konfigurieren
- WAN-Partner einrichten

8.4.1 Allgemeine Einstellungen

Hier finden Sie globale Parameter für IPX. Diese Einstellungen sind für alle IPX-Verbindungen von **X4000** gültig.

Die Konfiguration erfolgt in **IPX**:

Feld	Bedeutung
Local System Name	IPX-Systemname von X4000 in Großbuchstaben, Ziffern und , - : /.
Internal Network Number	X4000s interne Netzwerk-Nummer. Dieser Wert muß unter allen Netzwerk-Nummern einmalig sein und besteht standardmäßig aus den letzten vier Bytes von X4000s ►► MAC-Adresse . Ändern Sie diesen Wert nur, wenn er bereits an anderer Stelle im Netzwerk verwendet wird. Internal Network Number eines ►► Remote-IPX-Router den gleichen Wert hat.
enable IPX spoofing	Aktiviert bzw. deaktiviert NCP session watchdog spoofing und die Behandlung von "broadcast message waiting"-Paketen. Mögliche Werte: <input type="checkbox"/> <i>yes</i> : günstig für IPX-WAN-Verbindungen <input type="checkbox"/> <i>no</i>
enable SPX spoofing	Aktiviert bzw. deaktiviert SPX session watchdog spoofing. Mögliche Werte: <input type="checkbox"/> <i>yes</i> : günstig für SPX-Sessions über WAN-Verbindungen <input type="checkbox"/> <i>no</i>
NetBIOS Broadcast replication	Definiert, wie X4000 mit ►► NetBIOS -Paketen verfährt.

Tabelle 8-50: **IPX**

NetBIOS Broadcast replication enthält folgende Auswahlmöglichkeiten:

Mögliche Werte	Bedeutung
<i>yes</i>	Alle NetBIOS-Hosts im Netzwerk können aufeinander zugreifen, auch wenn häufig WAN-Verbindungen aufgebaut werden müssen. Kostenintensiv!
<i>no</i> (Standardwert) <i>on LAN only</i>	Nur NetBIOS-Hosts im LAN, für die keine WAN-Verbindungen aufgebaut werden müssen, können aufeinander zugreifen. Kostengünstig.

Tabelle 8-51: **NetBIOS Broadcast replication**

ToDo Gehen Sie folgendermaßen vor:

- Gehen Sie zu **IPX**.
- Geben Sie **Local System Name** ein.
- Geben Sie gegebenenfalls **Internal Network Number** ein (nur wenn nötig!).
- Aktivieren Sie gegebenenfalls **enable IPX spoofing**.
- Aktivieren Sie gegebenenfalls **enable SPX spoofing**.
- Wählen Sie **NetBIOS Broadcast replication** aus, z. B. *on LAN only*.
- Bestätigen Sie mit **SAVE**.

8.4.2 LAN-Schnittstelle konfigurieren

Konfigurieren Sie als nächstes die LAN-Schnittstelle von **X4000** zum IPX-Netzwerk. Die LAN-Schnittstelle ist die physikalische Schnittstelle zum lokalen Netzwerk. Im folgenden Menü teilen Sie dem Router die Netznummer des IPX-LANs mit, an dem er angeschlossen ist. Solange **X4000** diese Information nicht hat, kann er nicht aktiv am eigenen IPX-LAN teilnehmen.

Die Konfiguration erfolgt in **CM-100BT, FAST ETHERNET**:

Feld	Bedeutung
local IPX-NetNumber	Die IPX-Netzwerk-Nummer des LANs, an das X4000 angeschlossen ist.
Encapsulation	Definiert, welche Art von Header bei IPX-Paketen im angeschlossenen LAN verwendet werden. Mögliche Werte: <ul style="list-style-type: none">■ <i>none</i>■ <i>Ethernet II</i>■ <i>Ethernet 802.2 LLC</i>■ <i>Ethernet SNAP</i>■ <i>Ethernet NOVELL 802.3</i>

Tabelle 8-52: **CM-100BT, FAST ETHERNET**

ToDo Gehen Sie folgendermaßen vor:

- Gehen Sie zu **CM-100BT, FAST ETHERNET**.
- Geben Sie **local IPX-NetNumber** ein.
- Wählen Sie **Encapsulation** aus.
- Bestätigen Sie mit **SAVE**.

8.4.3 WAN-Partner einrichten

Wenn die Verbindung zu einem oder mehreren WAN-Partnern mit dem IPX-Protokoll realisiert wird, müssen Sie dafür beim WAN-Partner einige IPX-spezifische Einstellungen festlegen.

Die Konfiguration erfolgt in **WAN PARTNER** ► **EDIT** ► **IPX**:

Feld	Bedeutung
Enable IPX	Ermöglicht IPX für den WAN-Partner. Mögliche Werte: <input type="checkbox"/> <i>yes</i> <input type="checkbox"/> <i>no</i>
IPX NetNumber	IPX-Netzwerknummer der WAN-Verbindung. Wird von einigen IPX-Routern benötigt.
Send RIP/SAP Updates	Definiert, wie oft ►► RIP -(Routing Information Protocol) und SAP - (Service Advertising Protocol) Pakete von X4000 zum WAN-Partner geschickt werden. In IPX-Netzwerken werden RIP- und SAP-Pakete als ►► Broadcasts in verbundene Netze gesendet, um über aktuelle Routen und Dienste zu informieren. Der dadurch verursachte Datenfluß ist okay im LAN, für über WAN-Verbindungen angeschlossene Netze muß hier eine Einstellung zur Kontrolle des Datenflusses vorgenommen werden.
Update Time	Definiert, in welchen Zeitabständen periodische Updates gesendet werden.
Age Multiplier	Wenn während Update Time x Age Multiplier eingetragene Routen und Dienste nicht erneuert werden, werden sie gelöscht. Dies verhindert, daß sich unnötig viele Routen und Dienste ansammeln, die nicht genutzt werden.

Tabelle 8-53: **WAN PARTNER** ► **EDIT** ► **IPX**

Das Feld **Send RIP/SAP Updates** enthält folgende Auswahlmöglichkeiten, die mit Hilfe einer Tabelle erläutert werden:

Mögliche Werte für Send RIP/SAP Updates	Neue Verbindung wird geöffnet?	Aktualisierung der bestehenden Tabellen?	Periodische Aktualisierung?	Bemerkungen
<i>off</i>	nie	nein	nein	Alle Routen und Dienste müssen statisch eingetragen werden.
<i>triggered + piggyback (on changes, per. if link active)</i>	nur für Veränderungen	ja	ja	Dies ist die Standard-Einstellung, in den meisten Fällen ausreichend.
<i>triggered (on changes)</i>	nur für Veränderungen	ja	nein	Weniger Datenverkehr als <i>triggered + piggyback</i> , aber auch weniger zuverlässig.
<i>piggyback (only if link active)</i>	nie	ja	ja	Mindestens 1 stat. Route und 1 stat. Dienst müssen für den WAN-Partner eingetragen werden.
<i>passive triggered (on changes only if link active)</i>	nie	ja	nein	Mindestens 1 stat. Route und 1 stat. Dienst müssen für den WAN-Partner eingetragen werden.
<i>timed update (always)</i>	immer	ja	ja	Kostenintensiv!

Tabelle 8-54: **Send RIP/SAP Updates**

ToDo Gehen Sie folgendermaßen vor:

- Gehen Sie zu **WAN PARTNER** ➤ **EDIT** ➤ **IPX**.
- Wählen Sie **Enable IPX** aus: *yes*.
- Geben Sie **IPX NetNumber** ein.
- Wählen Sie **Send RIP/SAP Updates** aus.
- Geben Sie gegebenenfalls **Update Time** ein.

- Geben Sie gegebenenfalls **Age Multiplier** ein.
- Bestätigen Sie mit **OK**.
- Bestätigen Sie mit **SAVE**.

8.5 Bridging

X4000 unterstützt die Funktion Bridging. Die Beschreibung der Konfiguration von **X4000** als Bridge finden Sie in der [Software Reference](#).

8.6 Features mit Zusatzlizenz

In diesem Kapitel wird kurz dargestellt, welche Funktionen Sie auf **X4000** mit einer Zusatzlizenz freischalten können.

Die entsprechenden Zusatzlizenzen schalten Sie frei, indem Sie die erhaltenen Lizenzinformationen im Setup Tool Menü **LICENSES** hinzufügen (siehe [Kapitel 7.1.1, Seite 121](#)).

Für folgende Funktionen sind derzeit Zusatzlizenzen erhältlich:

- X.25
- Frame Relay
- OSPF
- VPN (Virtual Private Network)
- TAF (Token Authentication Firewall)

Detaillierte Informationen und Konfigurationshinweise (mit Beispielen) finden Sie in der [Extended Features Reference](#).

9 Konfiguration der Erweiterungs- und Ressourcenkarten mit dem Setup Tool

In diesem Kapitel erfahren Sie, welche Konfigurationsschritte Sie vornehmen können, wenn Sie Ihr **X4000**-Grundgerät mit einer Erweiterungskarte und gegebenenfalls mit Ressourcenkarten ausgestattet haben. Eingebaute Erweiterungs- bzw. Ressourcenkarten werden von X4000 beim Starten automatisch erkannt.

Für die Installation der Erweiterungs- und Ressourcenkarten beachten Sie bitte die mit den Karten mitgelieferte Einbauanleitung bzw. [Kapitel 3.2, Seite 53](#).



Tragen Sie gegebenenfalls erforderliche Lizenz(en) im Setup Tool ein (siehe [Kapitel 7.1.1, Seite 121](#)), bevor Sie mit der Konfiguration beginnen.

Das Kapitel ist folgendermaßen aufgebaut:

- WAN-Schnittstellenkarte für ISDN-BRI (Basic Rate Interface) ([Kapitel 9.1, Seite 288](#))
- WAN-Schnittstellenkarte für ISDN-PRI (Primary Rate Interface) und/oder G.703 ([Kapitel 9.2, Seite 292](#))
- LAN-Schnittstellenkarte für 10/100 MBit/s ([Kapitel 9.3, Seite 298](#))
- Ressourcenkarten mit Digitalmodems ([Kapitel 9.4, Seite 306](#))
- Ressourcenkarte zur Verschlüsselung und Kompression ([Kapitel 9.5, Seite 317](#))

9.1 WAN-Schnittstellenkarte für ISDN-BRI

Durch Installation einer BRI (Basic Rate Interface)-Erweiterungskarte können Sie **X4000** 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 9.4, Seite 306](#)) und/oder mit einer Ressourcenkarte zur Verschlüsselung und Kompression (siehe [Kapitel 9.5, Seite 317](#)) ausstatten.

9.1.1 Konfiguration mit dem Setup Tool

Im Setup-Tool-Hauptmenü werden die zusätzlichen Schnittstellen unter `Module:` folgendermaßen angezeigt:

X4000 Setup Tool		BinTec Communications AG MyRouter			
Licenses		System			
LAN:	CM-100BT, Fast Ethernet	Module: X4E-3BRI, ISDN S0			
WAN:	CM-1BRI, ISDN S0				
Serial-WAN:	CM-SERIAL, Serial				
WAN Partner					
IP	IPX	PPP	MODEM	ISDN	CAPI
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.

ToDo 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. Für detaillierte Erklärungen beachten Sie bitte [Kapitel 7.2.1, Seite 138](#).
- ▶ Wählen Sie **ISDN Switch Type** aus: *autodetect on bootup*.
Mit dieser Einstellung nutzt **X4000** 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*.
- ▶ Wählen Sie gegebenenfalls **D-Channel** aus.
- ▶ Wählen Sie **B-Channel 1** aus: z. B. *dialup*.
- ▶ Wählen Sie **B-Channel 2** aus: z. B. *dialup*.



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** ausgewählt haben und die Werte änderbar sind.

Incoming Call Answering Wenn über die ISDN-BRI-Schnittstelle Wählverbindungen aufgebaut werden sollen, teilen Sie X4000 als nächstes mit, wie auf eingehende Rufe über diese

Schnittstelle reagiert werden soll (bei einer Festverbindung sind diese Einstellungen nicht erforderlich):

- 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 142.

- 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. *091112330*.
- 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 gespeichert und werden in der Liste angezeigt.

Sie haben damit einer Ihrer Rufnummern (*0911 123 30*) einen möglichen Dienst (*PPP (routing)*) zugeordnet. D. h. wenn ein Daten-Ruf an die Called Party Number *0911 123 30* eingeht, wird er an den Dienst PPP (routing) weitergeleitet.

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

Damit haben Sie Incoming Call Answering für diese ISDN-BRI-Schnittstelle konfiguriert, **X4000** verteilt die eingehenden Rufe an die internen Dienste.

- 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 **X4000** Verbindungen zu Netzwerken oder Hosts außerhalb Ihres LANs herstellen zu können, müssen Sie die gewünschten Verbindungspartner als WAN-Partner auf **X4000** einrichten. Dies gilt sowohl für ausgehende Verbindungen, als auch für eingehende Verbindungen und Festverbindungen. Beachten Sie dazu [Kapitel 7.3, Seite 162](#).

9.2 WAN-Schnittstellenkarte für ISDN-PRI und/oder G.703

Die PRI (Primary Rate Interface)- bzw. G.703-Erweiterungskarte verfügt über zwei Ports mit jeweils zwei Buchsen (IN und OUT). Durch Installation der Erweiterungskarte können Sie **X4000** mit

- einer ISDN-PRI- und/oder einer G.703-Schnittstelle oder
- zwei ISDN-PRI-Schnittstellen oder
- zwei G.703-Schnittstellen

ausstatten. Die erforderlichen Lizenzen zum Freischalten der gewünschten Schnittstellen erhalten Sie von Ihrem Händler.

PRI Eine ISDN-PRI-Schnittstelle von X4000 können Sie an einen Primärmultiplexanschluß anschließen. Verbinden Sie dazu den NT (Network Termination)-Adapter Ihrer Telefongesellschaft mit der IN-Buchse eines per Lizenz freigeschalteten Ports. In Deutschland stehen Ihnen damit 30 B-Kanäle und 1 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 X4000 können Sie eine G.703-Festverbindung zu einem Verbindungspartner installieren. Verbinden Sie dazu ebenfalls den NT (Network Termination)-Adapter Ihrer Telefongesellschaft mit der IN-Buchse eines per Lizenz freigeschalteten Ports. Eine G.703-Festverbindung ist eine unstrukturierte Hochgeschwindigkeitsleitung mit bis zu 2 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 standardmäßig mit Hardware-Unterstützung für Verschlüsselung und Kompression ausgestattet ([Kapitel 9.5, Seite 317](#)) und kann optional mit bis zu zwei

Ressourcenkarten mit Digitalmodems ([Kapitel 9.4, Seite 306](#)) aufgerüstet werden.

9.2.1 Konfiguration mit dem Setup Tool

Im Setup-Tool-Hauptmenü werden die zusätzlichen Schnittstellen unter **Module**: folgendermaßen angezeigt:

X4000 Setup Tool		BinTec Communications AG MyRouter	
Licenses	System		
LAN:	CM-100BT, Fast Ethernet	Module: X4E-2PRI, ISDN S2M	
WAN:	CM-1BRI, ISDN S0		
Serial-WAN:	CM-SERIAL, Serial		
WAN Partner			
IP	IPX	PPP	MODEM ISDN CAPI
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.
ISDN Switch Type	Definiert das ISDN-►► Protokoll , das Ihnen Ihre Telefongesellschaft zur Verfügung stellt. Mögliche Werte: <ul style="list-style-type: none"> ■ <i>autodetect on bootup</i>: automatische D-Kanalerkennung (Standardeinstellung) ■ <i>Euro ISDN S2M user profile (TE)</i> ■ <i>Euro ISDN S2M network profile (NT)</i> ■ <i>leased line B1..B30</i> ■ <i>leased line, 1 Hyperchannel</i> ■ <i>leased line, chann. E1, 31 diff. endpoints</i>: Dieser Typ von Festverbindung wird in UK auch als "aggregated kilostream" bezeichnet. ■ <i>back to back</i>

Feld	Bedeutung
ISDN Line Framing	<p>Mögliche Werte:</p> <ul style="list-style-type: none"> ■ <i>standard (CRC4)</i> (Standardeinstellung) ■ <i>special (no CRC)</i> ■ <i>G.703</i>: Erforderlich, wenn Sie eine G.703-Festverbindung über die Schnittstelle einrichten wollen. <p>In den meisten Fällen wird für eine PRI-Schnittstelle die Standardeinstellung genutzt. In manchen Fällen in Schweden und Frankreich, wenn X4000 an eine TK-Anlage angeschlossen ist, ist die Einstellung <i>special (no CRC)</i> erforderlich.</p>
Clock Mode	<p>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.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ■ <i>extern</i> (Standardeinstellung): X4000 empfängt das Taktsignal ■ <i>intern</i>: X4000 gibt das Taktsignal

Tabelle 9-1: **X4E-2PRI, ISDN S2M** ➔ **UNIT 0** bzw. **X4E-2PRI, ISDN S2M** ➔ **UNIT 1**

ToDo Gehen Sie folgendermaßen vor:

- 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 **X4000** 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 X4000 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 X4000 als nächstes mit, wie auf eingehende Rufe über diese Schnittstelle reagiert werden soll (bei einer Festverbindung sind diese Einstellungen nicht erforderlich):

- 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 142.

- 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. *091112330*.
- 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 (0911 123 30) einen möglichen Dienst (0911 123 30) zugeordnet. D. h. wenn ein Daten-Ruf an die Called Party Number 0911 123 30 eingeht, wird er an den Dienst PPP (routing) weitergeleitet.
- Wiederholen Sie diese Schritte so oft, bis Sie allen Rufnummern die Dienste zugeordnet haben, die unter diesen Rufnummern erreichbar sein sollen.
Damit haben Sie Incoming Call Answering für diese ISDN-PRI-Schnittstelle konfiguriert, **X4000** verteilt die eingehenden Rufe an die internen Dienste.
- 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 **X4000** Verbindungen zu Netzwerken oder Hosts außerhalb Ihres LANs herstellen zu können, müssen Sie die gewünschten Verbindungspartner als WAN-Partner auf **X4000** einrichten. Dies gilt sowohl für ausgehende Verbindungen, als auch für eingehende Verbindungen und Festverbindungen. Beachten Sie dazu [Kapitel 7.3, Seite 162](#).

9.3 LAN-Schnittstellenkarte für 10/100 MBit/s

Durch Installation einer LAN-Erweiterungskarte können Sie **X4000** mit zwei zusätzlichen LAN-Schnittstellen ausstatten.

Die LAN-Erweiterungskarte können Sie optional mit einer Ressourcenkarte zur Verschlüsselung und Kompression (siehe [Kapitel 9.5, Seite 317](#)) ausstatten.

9.3.1 Konfiguration mit dem Setup Tool

Im Setup-Tool-Hauptmenü werden die zusätzlichen Schnittstellen unter `Module`: folgendermaßen angezeigt:

X4000 Setup Tool		BinTec Communications AG MyRouter	
Licenses	System		
LAN:	CM-100BT, Fast Ethernet	Module:	X4E-100BT, Fast Ethernet
WAN:	CM-1BRI, ISDN S0		
Serial-WAN:	CM-SERIAL, Serial		
WAN Partner			
IP	IPX	PPP	ISDN CAPI
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

ToDo Gehen Sie folgendermaßen vor, um die LAN-Schnittstelle(n) der Erweiterungskarte zu konfigurieren:

- 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 7.2.1, Seite 138](#).
- 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 gespeichert.

Weiterführende Konfiguration Wenn Sie das ➤➤ **Protokoll IPX** verwenden, finden Sie Erläuterungen zur Konfiguration der LAN-Schnittstelle für IPX in [Kapitel 8.4, Seite 278](#).

Informationen zu Bridging finden Sie in der [Software Reference](#).

9.3.2 Breitband-Internetzugang (ADSL) mit X4000 und LAN-Erweiterungskarte

BinTec Communications AG bietet mit X4000 das Protokoll PPP-over-Ethernet an. Dieses Protokoll wird benötigt, um z. B. Endgeräte über den T-DSL-Anschluß der Deutschen Telekom AG mit dem Internet zu verbinden und somit eine erhöhte Bandbreite zu erreichen.



Wenn Sie den ADSL-Anschluß eines anderen Providers nutzen, erkundigen Sie sich gegebenenfalls beim Provider über die zu beachtenden Besonderheiten Ihres ADSL-Anschlusses.

In [Kapitel 7.2.3, Seite 157](#) wird erläutert, wie Sie den T-DSL-Anschluß mit dem **X4000**-Grundgerät mit nur einer LAN-Schnittstelle nutzen können. Die dort beschriebenen Einschränkungen und Sicherheitsrisiken entfallen, wenn **X4000** mit einer LAN-Erweiterungskarte ausgestattet ist und damit mehrere LAN-Schnittstellen zur Verfügung stehen. In diesem Fall können Sie beispielsweise eine **X4000**-LAN-Schnittstelle für Ihr LAN und eine andere LAN-Schnittstelle für den Zugang zu T-DSL nutzen.

Beispielszenario

Folgendes Szenario dient als Beispielkonfiguration für die Einstellungen im Setup Tool. Der LAN-Anschluß wird über die LAN-Schnittstelle des **X4000**-Grundgeräts abgewickelt. Das ADSL-Modem wird mit einer der LAN-Schnittstellen der Erweiterungskarte verbunden.



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

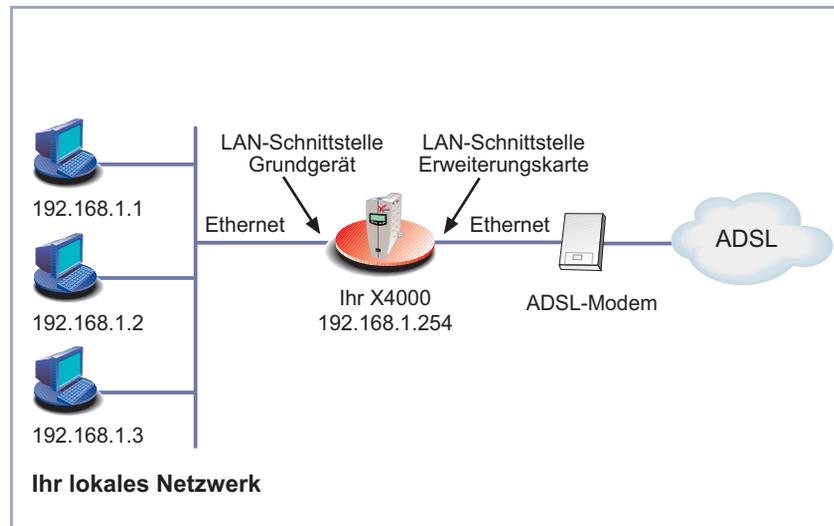


Bild 9-1: Beispielszenario

IP-Adresse konfigurieren Gehen Sie folgendermaßen vor, um die IP-Adresse von **X4000** festzulegen:

- Gehen Sie zu **CM-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 der 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 ADSL läuft.

Tabelle 9-2: **PPP**

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

- Wählen Sie Ihr **PPPoE Ethernet Interface** aus, z. B. **en2**.
- 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-Compression im Menü **WAN PARTNER** ➤ **ADD** ➤ **IP** ➤ **ADVANCED SETTINGS** nicht aktiviert ist. Ebenso dürfen die Funktionen IPX, 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.
Encapsulation	<p>Enkapsulierung. Definiert, wie die Datenpakete für die Übertragung zum WAN-Partner verpackt werden.</p> <p>Bei PPP-over-Ethernet: Hierbei sollte nur <i>PPP</i> ausgewählt werden.</p>
Calling Line Identification	<p>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 <i>Direction</i> im Untermenü WAN NUMBERS und kann hier nicht gesetzt werden.</p>

Tabelle 9-3: **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**.
- Gehen Sie zu **WAN PARTNER** ➤ **ADD** ➤ **PPP**.

WAN-Partner-PPP-Einstellungen

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 (hier: 000460004256) T-Online-Nr. = Telefonnummer (hier: 091169386) Mitben.-Nr. = vierstellige Mitbenutzernummer (hier: 0001) Die T-Online-Nummer und die Mitbenutzernummer müssen durch # getrennt werden, wenn die T-Online-Nummer weniger als 12 Stellen hat.
PPP Password	Ihr T-Online Paßwort.
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 9-4: **WAN PARTNER** ➤ **ADD** ➤ **PPP**

- Machen Sie unter **Partner PPP ID** keine Eintragung.
- Tragen Sie **Local PPP ID** ein,
z. B. **000460004256091169386#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	Hier können Sie das Layer 1 Protocol des ISDN-B-Kanals, das X4000 für Verbindungen zum WAN-Partner nutzen soll, definieren. Für den Zugang zu T-DSL muß hier PPP over Ethernet (PPPoE) ausgewählt werden.

Tabelle 9-5: **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 X4000 ein Transit-Network zum WAN-Partner nutzt. Die IP-Adresse wird dynamisch zugewiesen, wenn <i>dynamic client</i> ausgewählt ist.

Tabelle 9-6: **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 9-7: **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, daß

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

Folgendes Feld ist hierbei interessant:

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 9-8: **IP** ➤ **NAT**

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

9.4 Ressourcenkarte mit Digitalmodems

ISDN-BRI- und ISDN-PRI-/G.703-Erweiterungskarten (siehe [Kapitel 9.1, Seite 288](#) bzw. [Kapitel 9.2, Seite 292](#)) können zusätzlich mit Ressourcenkarten mit Digitalmodems ausgestattet werden.

Ressourcenkarten mit Digitalmodems sind in unterschiedlichen Ausführungen erhältlich:

- XTR-S: Ressourcenkarte mit 8 Digitalmodems
- XTR-M: Ressourcenkarte mit 12 Digitalmodems
- XTR-L: Ressourcenkarte mit 30 Digitalmodems

Ausgerüstet mit Ressourcenkarte(n) mit Digitalmodems für analoge Daten- und Faxverbindungen kann X4000 genutzt werden als

- Remote-Access-Server für ISDN- und GSM-Verbindungen sowie für analoge Verbindungen (Dial-In)
- Fax-Gateway (beachten sie hierfür bitte künftige Software-Releases und Release Notes)



Bei Verwendung einer Erweiterungskarte mit Ressourcenkarte(n) im X4000-Einbaugerät empfiehlt BinTec Communications AG die Verwendung der optional erhältlichen Lüfterkassette.

9.4.1 X4000 mit Digitalmodems als Remote-Access-Server

Ausgerüstet mit Digitalmodems kann X4000 für Dial-in-Verbindungen genutzt werden, z. B von Home-Office-Mitarbeitern mit analogen Modems oder von Außendienstmitarbeitern mit Laptop, Handy und Modem.

X4000 nutzt die Digitalmodems der Ressourcenkarte(n) als Modem-Pool und verwendet bei einer eingehenden Dial-In-Verbindung immer dynamisch das nächste verfügbare Modem.

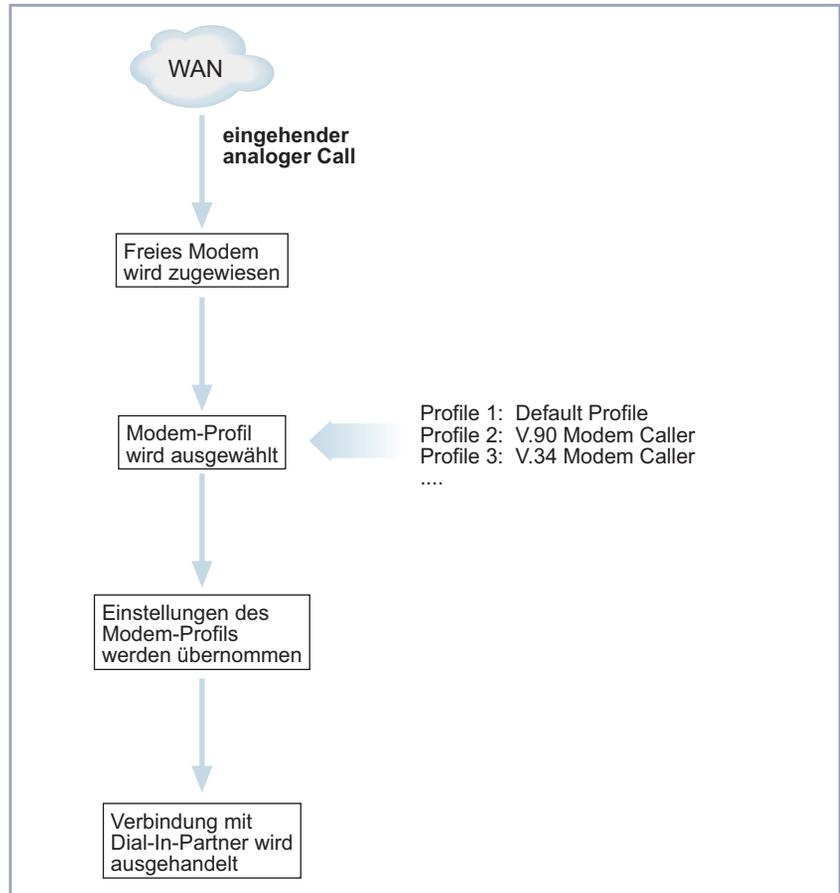


Bild 9-2: Dial-In auf X4000 mit Digitalmodems

Die Modems (z. B. 30 Modems bei einer Ressourcenkarte XTR-L) müssen nicht einzeln konfiguriert werden, da X4000 ein flexibles Konzept von Modem-Profilen verwendet. Bis zu acht Modem-Profilen können auf X4000 im Menü **MODEM ► PROFILE CONFIGURATION** konfiguriert werden, das tatsächlich genutzte Modem übernimmt beim Verbindungsaufbau jeweils dynamisch die Einstellungen des passenden Modem-Profils. Ein Modem-Profil definiert die Einstellungen des Modems, die für eine Verbindung mit der Gegenstelle benötigt werden, z. B. automatische Baudraten-Aushandlung, Kompression und maximale bzw. minimale Baud-Rate. Durch die Erstellung von mehreren Modem-

Profilen 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 Modem-Profil für einen eingehenden Call verwendet werden soll. Falls dem Einwählenden kein Modem-Profil zugewiesen wurde oder der Anrufende nicht authentisiert werden kann, verwendet das Modem 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 Modem-Profilen können Sie User-Gruppen definieren, so daß die einwählenden Dial-In-Verbindungspartner optimale Modemeinstellungen auf X4000 vorfinden.

Beispielszenario Ein typisches Szenario, z. B. für einen Internet Service Provider, könnte folgendermaßen aussehen:

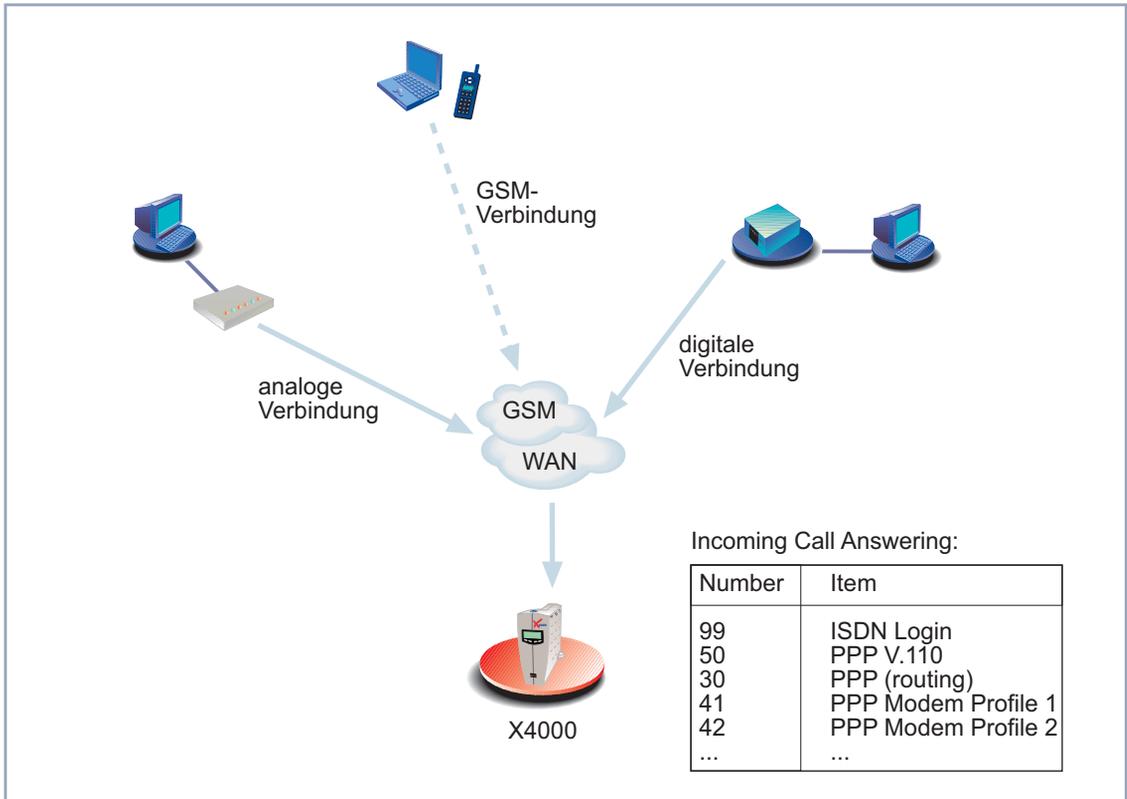


Bild 9-3: Szenario für Dial-In

- 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).
- Dial-In-User, die eine ISDN-Verbindung nutzen, verwenden 0911 123 30.
- Dial-In-User, die sich mit einem Handy über eine GSM-Verbindung einwählen, verwenden 0911 123 50.
- Eingehende Rufe an die Rufnummer 0911 123 99 werden an den Dienst ISDN-Login weitergeleitet.

Konfiguration mit dem Setup Tool

Wenn X4000 mit einer Ressourcenkarte mit Digitalmodems ausgestattet ist, erscheint das Menü **MODEM** im Setup-Tool-Hauptmenü:

X4000 Setup Tool		BinTec Communications AG MyRouter	
Licenses		System	
LAN:	CM-100BT, Fast Ethernet	Module: X4E-3BRI, ISDN S0	
WAN:	CM-1BRI, ISDN S0		
Serial-WAN: CM-SERIAL, Serial			
WAN Partner			
IP	IPX	PPP	MODEM ISDN CAPI
Configuration Management			
Monitoring and Debugging			
Exit			

Im Menü **MODEM** werden die Modem-Profile, deren Einstellungen die Digitalmodems auf X4000 nutzen, festgelegt.

Allgemeine Vorgehensweise bei der Konfiguration von Dial-In-Verbindungen:

1. Definieren Sie zunächst die Einstellungen für Modem Profile 1 in **MODEM ► PROFILE CONFIGURATION**.
2. Definieren Sie gegebenenfalls weitere Modem Profiles 2 ... 8 in **MODEM ► PROFILE CONFIGURATION**.
3. Regeln Sie mit den Einstellungen für Incoming Call Answering die Verwendung der Modem-Profile in Abhängigkeit vom einwählenden Verbindungspartner, z. B. in **X4E-3BRI, ISDN S0 ► UNIT 0 ► INCOMING CALL ANSWERING**.
4. Konfigurieren Sie für jeden Dial-In-User einen WAN-Partner-Eintrag in **WAN PARTNER**.

Die Menüs **MODEM** ► **PROFILE CONFIGURATION** ► **PROFILE 1 ... 8** enthalten folgende Felder:

Feld	Bedeutung
Name	Profile 1 ... 8 wird angezeigt.
Description	Frei wählbare Beschreibung des Modem-Profiles.
Modulation	<p>Legt den zu benutzenden Modem-Standard fest. Der gewählte Modem-Standard muß vom analogen Modem der Gegenstelle unterstützt werden.</p> <p>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.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ■ V.90 ■ V.34bis ■ V.34 ■ V.32bis ■ V.32 ■ V.23 ■ V.22bis ■ V.22 ■ V.21
Error Correction	<p>Legt die zu benutzende Fehlerkorrektur fest.</p> <p>Mögliche Werte siehe Tabelle 9-10, Seite 314.</p>

Feld	Bedeutung
Automode	<p>Legt fest, ob die dynamische Aushandlung von Parametern für Baudraten und Modem-Standards mit dem Dial-In-User erlaubt ist.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ■ <i>on</i> (Standardwert): Aushandlung ist erlaubt. ■ <i>off</i>: Eingestellte Werte werden immer verwendet.
Min Bps	<p>Legt die minimale Baudrate fest, die mit dem Modem-Profil genutzt werden kann. Jede Geschwindigkeit, die von dem unter Modulation eingestellten Modem-Standard unterstützt wird, kann hier eingestellt werden.</p> <p>Die Verbindung wird abgebaut, wenn mit der Gegenstelle nur eine Baudrate ausgehandelt werden kann, die kleiner als der hier eingestellte Wert ist.</p> <p>Skalierbar von <i>300</i> (Standardwert) bis <i>56000</i>.</p>
Max Receive Bps	<p>Legt die maximale Baudrate für eingehende Daten ("upstream") fest, die mit dem Modem-Profil genutzt werden kann. Jede Geschwindigkeit, die von dem unter Modulation eingestellten Modem-Standard unterstützt wird, kann hier eingestellt werden.</p> <p>Der unter Max Transmit Bps eingestellte Wert wird hier verwendet, falls dieser Wert kleiner ist als der hier eingestellte.</p> <p>Skalierbar von <i>300</i> bis <i>56000</i>, Standardwert: <i>33600</i>.</p>

Feld	Bedeutung
Max Transmit Bps	Wird nur verwendet, wenn Modulation = V.90 . Legt die maximale Baudrate für ausgehende Daten ("downstream") fest, die mit dem Modem-Profil genutzt werden kann. Skalierbar von 300 bis 56000, Standardwert: 33600.
V.42bis Compression	Legt fest, ob V.42bis-Kompression für eine Verbindung ausgehandelt werden darf. Mögliche Werte: <ul style="list-style-type: none"> ■ <i>auto</i>: Aushandlung wird erlaubt. ■ <i>off</i>: V.42bis-Kompression wird nicht genutzt.
MNP5 Compression	Legt fest, ob MNP5-Kompression für eine Verbindung ausgehandelt werden darf. Mögliche Werte: <ul style="list-style-type: none"> ■ <i>auto</i>: Aushandlung wird erlaubt. ■ <i>off</i>: MNP5-Kompression wird nicht genutzt.

Tabelle 9-9: Menü **MODEM** ➤ **PROFILE CONFIGURATION** ➤ **PROFILE 1 ... 8**

Das Feld **Error Correction** enthält folgende Auswahlmöglichkeiten:

Mögliche Werte	Bedeutung
<i>none</i>	Fehlerkorrektur wird nicht genutzt.
<i>required</i>	Als Fehlerkorrektur wird zunächst LAPM und anschließend MNP4 versucht. Schlägt beides fehl, beendet das Modem die Verbindung.
<i>auto</i> (Standardwert)	Als Fehlerkorrektur wird zunächst LAPM und anschließend MNP5 versucht. Schlägt beides fehl, wird keine Fehlerkorrektur genutzt. Diese Einstellung sollte i. a. gewählt werden, außer für Dial-In-User mit Modems, die lediglich veraltete Standards wie V.23, V.22bis oder V.21 unterstützen.
<i>LAPM</i>	LAPM (Link Access Protocol for Modems) wird genutzt. Wenn dies fehlschlägt, beendet das Modem die Verbindung.
<i>MNP</i>	MNP4 (Microcom Networking Protocol) wird genutzt. Wenn dies fehlschlägt, beendet das Modem die Verbindung.

Tabelle 9-10: **Error Correction**

ToDo Gehen Sie im Detail folgendermaßen vor:

- Gehen Sie zu **MODEM** ➤ **PROFILE CONFIGURATION**.
 - Wählen Sie **PROFILE 1** aus und bestätigen mit der **Eingabetaste**.
- Modem Profile 1 konfigurieren**
- Geben Sie **Description** ein, z. B. *Standardmodemprofil*.
 - Wählen Sie **Modulation** aus, z. B. *V.34*
 - Wählen Sie **Error Correction** aus, z. B. *auto*.
 - Wählen Sie **Automode** aus, z. B. *on*.
 - Wählen Sie **Min Bps** aus, z. B. *2400*.
 - Wählen Sie **Max Receive Bps** aus, z. B. *33600*.

- Wählen Sie gegebenenfalls **Max Transmit Bps** aus, z. B. *33600*.
 - 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 Modem-Profile. Beachten Sie dabei [Tabelle 9-11, Seite 316](#).
- Incoming Call Answering**
- Gehen Sie folgendermaßen vor, um die definierten Modem-Profile den Dial-In-Usern zuzuordnen (die Beispielwerte sind dem Szenario in [Bild 9-3, Seite 309](#) entnommen):
- Gehen Sie zu **X4E-3BRI, ISDN SO ▶ UNIT 0 ▶ INCOMING CALL ANSWERING**, wenn Sie eine über die erste Schnittstelle einer ISDN-BRI-Erweiterungskarte eingehende Dial-In-Verbindungen 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. *091112342*.
 - Wählen Sie **Mode** aus, z. B. *right to left*.
 - Wählen Sie **Bearer** aus, z. B. *any*.
 - Bestätigen Sie mit **SAVE**.
 - Fügen Sie gegebenenfalls weitere Einträge hinzu.
- WAN-Partner**
- Gehen Sie folgendermaßen vor, um für die Dial-In-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 7.3, Seite 162](#), 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 X4000 zu verwendende Rufnummer ein, z. B. *09117890*.
- Wählen Sie **Direction** aus, z. B. *outgoing*.
- 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 177).
- Bestätigen Sie mit **SAVE**.
Der WAN-Partner-Eintrag wird angezeigt.
- Zur Einrichtung weiterer WAN-Partner gehen sie analog vor.

Tabelle 9-11, Seite 316 zeigt anhand eines allgemeinen Beispiels, wie Sie die Modem-Profile auf X4000 auf sinnvolle Weise nutzen könnten:

Profile	Modulation	Error Correction	Automode	Min Bps	Max Receive Bps	Max Transmit Bps	v.42bis	MNP5
Profile 1	V.34	auto	on	2400	33600	33600	auto	auto
Profile 2	V.90	auto	on	28800	31200	50000	auto	auto
Profile 3	V.90	auto	on	28800	31200	44000	auto	auto
Profile 4	V.90	auto	on	14400	31200	40000	auto	auto
Profile 5	V.32bis	auto	on	4800	14400	14400	auto	auto
Profile 6	V.32	auto	on	4800	9600	9600	auto	auto
Profile 7	V.23	auto	on	300	1200	1200	auto	auto
Profile 8	V.22bis	auto	on	300	2400	2400	auto	auto

Tabelle 9-11: Standard-Set von Modem-Profilen

9.5 Ressourcenkarte zur Verschlüsselung und Kompression

Die ISDN-PRI- bzw. G.703-Erweiterungskarte ist im Auslieferungszustand standardmäßig mit Hardwareunterstützung 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 hardwaremäßig STAC-Kompression und symmetrische Verschlüsselungsverfahren (DES, 3DES, CAST, Twofish, Blowfish). Somit kann die zur Verfügung stehende Bandbreite maximal ausgenutzt und die Verbindungskosten gesenkt werden, ohne die Performance von X4000 zu beeinträchtigen.



Bei Verwendung einer Erweiterungskarte mit Ressourcenkarte(n) im X4000-Einbaugerät empfiehlt BinTec Communications AG die Verwendung der optional erhältlichen Lüfterkassette.

9.5.1 Konfiguration mit dem Setup Tool

Die Konfiguration von STAC-Kompression und Verschlüsselung erfolgt in gewohnter Weise im Setup-Tool-Menü **WAN PARTNER** ► **EDIT** (siehe [Kapitel 8.2.9, Seite 239](#) bzw. [Kapitel 10.3.1, Seite 370](#)).

10 Konfiguration von Sicherheitsfunktionen und Firewall

SAFERNET BinTec Communications AG ermöglicht mit **X4000** eine hohe Sicherheit Ihres Netzwerks und Ihrer Verbindungen. Die verfügbaren Sicherheits-Funktionen (SAFERNET) erlauben das Überwachen von Aktivitäten über den Router und eine wirksame Zugangs- bzw. Abhörsicherung. Die erforderlichen Konfigurationsschritte werden in diesem Kapitel dargestellt.

Manches können Sie nicht mit Hilfe des Setup Tools konfigurieren, sondern nur durch direktes Eintragen in ►► **MIB**-Tabellen. Die entsprechenden Tabellen bzw. Variablen werden im jeweiligen Abschnitt genannt.



MIB-Einträge können Sie entweder durch Kommandos in der ►► **SNMP-Shell** oder durch externe SNMP-Manager, z. B. Configuration Manager, vornehmen. Eine Beschreibung der SNMP-Kommandos finden Sie in der [Software Reference](#).

Das Kapitel ist folgendermaßen aufgebaut:

- Überwachen von Aktivitäten ([Kapitel 10.1, Seite 320](#))
- Zugangssicherung ([Kapitel 10.2, Seite 338](#))
- Abhörsicherung ([Kapitel 10.3, Seite 370](#))
- Besonderheiten ([Kapitel 10.4, Seite 374](#))
- Checkliste ([Kapitel 10.5, Seite 376](#))

10.1 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 Communications AG eine Vielzahl an Möglichkeiten zur Verfügung:

- Syslog-Messages ([Kapitel 10.1.1, Seite 320](#))
- Monitorfunktionen im Setup Tool ([Kapitel 10.1.2, Seite 325](#))
- Credits Based Accounting System (Taschengeldkonto) ([Kapitel 10.1.3, Seite 328](#))
- HTTP-Statusseite ([Kapitel 10.1.4, Seite 332](#))
- Java-Statusmonitor ([Kapitel 10.1.5, Seite 334](#))
- Activity Monitor ([Kapitel 10.1.6, Seite 334](#))

10.1.1 Syslog-Messages

Alle wesentlichen Ereignisse auf **X4000s** 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 **X4000** in einer Liste von einstellbarer Länge gespeichert. Alle Informationen können und sollten zur Speicherung und Weiterverarbeitung an einen oder mehrere externe Rechner weitergeleitet werden, z. B. an den Rechner des System-Administrators. Auf **X4000** 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**

Feld	Bedeutung
Syslog output on serial console	<p>Ermöglicht die Anzeige von Syslog-Messages auf dem mit der seriellen Schnittstelle von X4000 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:</p> <ul style="list-style-type: none"> <input type="checkbox"/> <i>yes</i> <input type="checkbox"/> <i>no</i>
Message level for the syslog table	<p>Spezifiziert die Priorität der intern aufzuzeichnenden Syslog-Messages. Mögliche Werte:</p> <ul style="list-style-type: none"> <input type="checkbox"/> <i>emerg</i>: Emergency Messages (höchste Priorität) <input type="checkbox"/> <i>alert</i>: Alert Messages <input type="checkbox"/> <i>crit</i>: Critical Messages <input type="checkbox"/> <i>err</i>: Error Messages <input type="checkbox"/> <i>warning</i>: Warning Messages <input type="checkbox"/> <i>notice</i>: Notice Message <input type="checkbox"/> <i>info</i>: Info Messages <input type="checkbox"/> <i>debug</i>: Debug Messages (niedrigste Priorität) <p>Nur Syslog-Messages mit höherer oder gleicher Priorität wie angegeben werden intern aufgezeichnet.</p>
Maximum Number of Syslog Entries	<p>Maximale Anzahl an Syslog-Messages, die auf X4000 intern gespeichert werden (Wertebereich: <i>0 ... 100</i>).</p>

Tabelle 10-1: **SYSTEM**

Feld	Bedeutung
Log Host	➤➤ IP-Adresse des Hosts, zu dem Syslog-Messages weitergeleitet werden.
Level	Priorität der zu Log Host zu schickenden Syslog-Messages. Entspricht Message level for the syslog table in SYSTEM .
Facility	Syslog-Facility auf Log Host . Nur erforderlich, wenn der Log Host ein Unix-Rechner ist.
Type	Nachrichtentyp. Mögliche Werte: <ul style="list-style-type: none"> ■ <i>all</i>: Alle Messages. ■ <i>system</i>: Syslog-Messages außer ➤➤ Accounting-Messages. ■ <i>accounting</i>: Accounting-Messages.

Tabelle 10-2: **SYSTEM** ➤ **EXTERNAL SYSTEM LOGGING**

Feld	Bedeutung
IP Accounting	Ermöglicht Speichern von Accounting-Messages für ➤➤ TCP -, ➤➤ UDP - und ICMP-Sitzungen. Mögliche Werte: <i>on</i> , <i>off</i> .

Tabelle 10-3: **CM-100BT**, **FAST ETHERNET** ➤ **ADVANCED SETTINGS**

Feld	Bedeutung
IP Accounting	Ermöglicht Speichern von Accounting-Messages für ➤➤ TCP -, ➤➤ UDP - und ICMP-Sitzungen. Mögliche Werte: <i>on</i> , <i>off</i> .

Tabelle 10-4: **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 **Syslog output on serial console** aus.
- Wählen Sie **Message level for the syslog table** aus.
- Geben Sie **Maximum Number of Syslog Entries** ein.
- Gehen Sie zu **SYSTEM** ➤ **EXTERNAL SYSTEM LOGGING**, um Syslog-Messages an externe Hosts weiterzuleiten:
- Wählen Sie einen bestehenden Eintrag aus und bestätigen Sie mit der **Eingabetaste** oder fügen Sie einen neuen Eintrag mit **ADD** hinzu.
- Geben Sie **Log Host** ein.
- Wählen Sie **Level** aus.
- Wählen Sie **Facility** aus.
- Wählen Sie **Type** aus.

IP-Accounting LAN-seitig Gehen Sie folgendermaßen vor, um IP-Accounting für einen LAN-Partner zu aktivieren. Damit werden auf **X4000** 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 **X4000** 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 **X4000** intern gespeicherten Syslog-Messages angezeigt:

X4000 Setup Tool		BinTec Communications AG
[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 **X4000** zu löschen.

Zur Interpretation von Syslog-Messages: Siehe [Software Reference](#).

10.1.2 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
- Schnittstellen-Statistik (vergleichende Darstellung mehrerer Schnittstellen)
- ➤➤ TCP/IP-Statistik
- Syslog-Messages (siehe [Kapitel 10.1.1, Seite 320](#))

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.

X4000 Setup Tool			BinTec Communications AG		
[MONITOR][ISDN CALLS]: ISDN Monitor - Calls			MyRouter		
Dir	Remote Name/Number	Charge	DurationeStack	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 **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.
- Wählen Sie **c**, um wieder die Liste der bestehenden ISDN-Verbindungen anzuzeigen.

Taschengeldkonto Gehen Sie folgendermaßen vor, um den Stand des Taschengeldkontos ([Kapitel 10.1.3, Seite 328](#)) 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.

X4000 Setup Tool		BinTec Communications AG	
[MONITOR][CREDITS][STAT]: Monitor isdnlogin Credits		MyRouter	
Time till end of measure interval(sec)	Total	Maximum	% reached
	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		
EXIT			

Informationen über die Konfigurierung des Taschengeldkontos finden Sie in [Kapitel 10.1.3, Seite 328](#).

Schnittstellen-Statistik

Gehen Sie folgendermaßen vor, um aktuelle Werte und Aktivitäten der **X4000**-Schnittstellen anzuzeigen:

➤ Gehen Sie zu **MONITORING AND DEBUGGING** ➤ **INTERFACES**.

Die Werte von zwei Schnittstellen werden nebeneinander angezeigt.

X4000 Setup Tool		BinTec Communications AG	
[MONITOR][INTERFACE]: Interface Monitoring		MyRouter	
Interface Name	en1	PROVIDER	
Operational Status	up	dormant	
	total	per second	total per second
Received Packets	5512	0	0
Received Octets	920664	0	0
Received Errors	0		
Transmit Packets	9	0	0
Transmit Octets	1193	0	0
Transmit Errors	0		
Active Connections	N/A	0	
Duration	N/A	0	
EXIT	EXTENDED	EXTENDED	
Use <Space> to select			

➤ Wählen Sie unter **Interface Name** die anzuzeigende Schnittstelle aus.

- Wählen Sie **EXTENDED**, um zusätzliche Informationen anzuzeigen. Anschließend können Sie unter **Operation** den Status der Schnittstelle verändern und die Eingabe mit **START OPERATION** bestätigen.

TCP/IP-Statistik Gehen Sie folgendermaßen vor, um eine Statistik der Verbindungen mit den
 ➤➤ **Protokollen ICMP**, ➤➤ **IP**, UDP und TCP anzuzeigen:

- Gehen Sie zu **MONITORING AND DEBUGGING** ➤ **TCP/IP**.

Die Statistik für IP-Verbindungen wird angezeigt. Die Bedeutung der MIB-Variablen finden Sie in der [MIB Reference](#).

X4000 Setup Tool		BinTec Communications AG	
[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			

- 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 TCP darzustellen.

10.1.3 Credits Based Accounting System (Taschengeldkonto)

ISDN-Gebühren Mit dem Taschengeldkonto von **X4000** 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 **X4000** 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 **X4000** steht Ihnen wieder das gesamte Konto zur Verfügung.

Die Konfiguration erfolgt in **ISDN** ► **CREDITS**:

Feld	Bedeutung
Surveillance	Definiert, ob das Taschengeldkonto für das jeweilige Subsystem aktiviert werden soll. Mögliche Werte: <i>off</i> , <i>on</i> . Bei <i>on</i> 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 <i>on</i> 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 <i>on</i> 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 <i>on</i> aktivieren, können Sie den gewünschten Wert in der darunterliegenden Zeile eintragen.
Maximum Time for Incoming Connections (sec)	Maximal erlaubte Zeit in Sekunden für eingehende Verbindungen während Measure Time (sec) . Wenn Sie diese Einstellung mit <i>on</i> aktivieren, können Sie den gewünschten Wert in der darunterliegenden Zeile eintragen.

Feld	Bedeutung
Maximum Time for Outgoing Connections (sec)	Maximal erlaubte Zeit in Sekunden für ausgehende Verbindungen während Measure Time (sec) . Wenn Sie diese Einstellung mit <i>on</i> 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 <i>on</i> 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 <i>on</i> aktivieren, können Sie den gewünschten Wert in der darunterliegenden Zeile eintragen.

Tabelle 10-5: **ISDN** ➔ **CREDITS**

ToDo Gehen Sie folgendermaßen vor:

- Gehen Sie zu **ISDN** ➔ **CREDITS**.
- Wählen Sie **Subsystem** aus und bestätigen Sie mit der **Eingabetaste**.
- Wählen Sie **Surveillance** aus: *on*, wenn Sie das Taschengeldkonto für das gewählte **Subsystem** nutzen wollen.
- Geben Sie **Measure Time (sec)** ein, z. B. *86400* (= 24 Stunden).
- Aktivieren Sie gegebenenfalls **Maximum Number of Incoming Connections** und tragen Sie 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**.

10.1.4 HTTP-Statusseite

Jeder BinTec-Router verfügt über eine interne Homepage, die sog. HTTP-Statusseite. Damit können Sie mit Hilfe eines Internet Browsers (z. B. Netscape Navigator, Internet Explorer) den Status von **X4000** anzeigen. So können alle Benutzer des **X4000**-LANs, sofern Sie das Paßwort des Benutzernamens `http` kennen, Einblick in den Status des Routers nehmen.



Bitte beachten Sie: HTTP-Seiten werden meist im Cache-Speicher des Browsers gehalten, so daß sie evtl. durch andere Benutzer am selben Arbeitsplatz gelesen werden können und evtl. auch auf beteiligten Proxy- ➤ ➤ **Servern** sichtbar sind.

- Geben Sie die URL `http://<System Name>` in Ihren Browser ein. (Anstatt des Namens können Sie auch die IP-Adresse von **X4000** eingeben.) Die HTTP-Statusseite des BinTec-Routers mit dem Systemnamen `<System Name>` bzw. mit der angegebenen IP-Adresse wird angezeigt.

Die HTTP-Statusseite enthält drei Tabellen:

- System description:
Hier sind neben der Version der System-Software Informationen aus der MIB-Tabelle **system** aufgelistet, wie **System Name** und **Contact**. Wenn unter **Contact** eine gültige E-Mail-Adresse angegeben ist, ist diese unterstrichen dargestellt.

- **Software options:**
Hier sind Informationen aus der MIB-Tabelle **biboAdmLicInfoTable** aufgelistet, der Status von **X4000**'s Subsystemen wird angezeigt.
- **Hardware Interfaces:**
Hier werden die LAN- und WAN-Schnittstellen von **X4000** angezeigt. Die dritte Spalte der Tabelle informiert über den aktuellen Status der physikalischen Schnittstellen.

Die HTTP-Statusseite enthält einige Links:

- **update**
Klicken Sie **update**, um die Statusseite zu aktualisieren.
- **login**
Klicken Sie **login**, um sich auf den dazugehörigen BinTec-Router via **>> telnet** einzuloggen.
- **http://www.bintec.de**
Damit gelangen Sie auf BinTecs WWW-Server mit den neuesten Informationen zu den Produkten und aktueller System-Software und Dokumentation für **X4000**.
- **system tables**
Klicken Sie auf **system tables**, um eine Liste mit allen MIB-Tabellen von **X4000** anzuzeigen. Durch Anklicken eines Tabellen-Namen werden die darin enthaltenen Variablen aufgelistet.



Wenn Sie die Anzeige von **X4000**'s HTTP-Statusseite verhindern möchten, dann tragen Sie als Portnummer des http-Ports 0 ein:

- Gehen Sie zu **IP** ➤ **STATIC SETTINGS**.
- Geben Sie **HTTP TCP port** ein: **0**.
- Bestätigen Sie mit **SAVE**.

10.1.5 Java-Statusmonitor

Mit dem Java Statusmonitor steht Ihnen eine weitere Möglichkeit zur Verfügung, mit einem Internet-Browser Informationen über **X4000** darzustellen. Folgende Daten sind damit abrufbar:

- Statische Informationen wie Systemname des BinTec-Routers und Software-Version
- Datenfluß über die einzelnen Schnittstellen
- Verbindungen zu WAN-Partnern

Wenn Sie den JAVA Statusmonitor zusammen mit der BRICKware installiert haben (siehe [Kapitel 6.2, Seite 113](#)), können Sie ihn folgendermaßen starten:

- Klicken Sie im Windows-Startmenü auf **Program** ➤ **BRICKware** ➤ **Java Status Monitor**.

Der JAVA Statusmonitor öffnet sich mit Ihrem Standard-Browser.

Weitere Erklärungen zum JAVA Statusmonitor finden Sie in [BRICKware for Windows](#).

10.1.6 Activity Monitor

Wozu? Mit dem Activity Monitor können Windows-Nutzer die Aktivitäten von **X4000** 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 **X4000** ist möglich.

Wie funktioniert's? Ein Status-Daemon sammelt Informationen über **X4000** und überträgt sie in Form von UDP-Paketen zur Broadcast-Adresse des LAN (Standardeinstellung) oder zu einer explizit eingetragenen IP-Adresse. Ein Paket pro **X4000**-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 Activity Monitor zu aktivieren, müssen Sie

- die zu überwachenden **X4000**(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	<p>IP-Adresse, zu der X4000 die UDP-Pakete schickt.</p> <p>Mit dem Standardwert <i>255.255.255.255</i> wird die Broadcast-Adresse der ersten LAN-Schnittstelle verwendet.</p> <p>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 (standardmäßig wird alle 5 Sekunden ein Paket geschickt).</p>
Client UDP Port	<p>Portnummer für Activity Monitor (Standardwert: <i>2107</i>, registriert durch IANA - Internet Assigned Numbers Authority).</p>
Type	<p>Art der Informationen, die mit den UDP-Paketen zur Windows-Anwendung geschickt werden. Mögliche Werte:</p> <ul style="list-style-type: none"> ■ <i>off</i>: deaktiviert Activity Monitor (Standardwert) ■ <i>physical</i>: nur Informationen über physikalische Schnittstellen ■ <i>physical_virt</i>: Informationen über physikalische und virtuelle Schnittstellen
Update Interval (sec)	<p>Update-Intervall in Sekunden. Mögliche Werte: <i>0</i> bis <i>60</i> (Standardwert: <i>5</i>).</p>

Tabelle 10-6: **SYSTEM** ► **EXTERNAL ACTIVITY MONITOR**



Die Einteilung der **X4000**-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**.

10.2 Zugangssicherung

Es gibt einige Möglichkeiten, das Einloggen und Zugreifen auf **X4000** nur autorisierten Benutzern zu ermöglichen:

- Anmelden ([Kapitel 10.2.1, Seite 338](#))
- Überprüfen der eingehenden Rufnummer (CLID) ([Kapitel 10.2.2, Seite 339](#))
- Authentisierung von PPP-Verbindungen ([Kapitel 10.2.3, Seite 340](#))
- Callback ([Kapitel 10.2.4, Seite 341](#))
- Closed User Group ([Kapitel 10.2.5, Seite 343](#))
- Zugriff auf Remote-CAPI ([Kapitel 10.2.6, Seite 343](#))
- Network Address Translation (NAT) ([Kapitel 10.2.7, Seite 344](#))
- Filter ([Kapitel 10.2.8, Seite 349](#))
- Lokale Filter ([Kapitel 10.2.9, Seite 363](#))
- Backroute Verification ([Kapitel 10.2.10, Seite 367](#))
- TAF ([Kapitel 10.2.11, Seite 368](#))
- Extended IP-Routing (XIPR) ([Kapitel 10.2.12, Seite 368](#))

10.2.1 Anmelden

Paßwort Das Anmelden auf **X4000** kann wie in [Kapitel 4.2, Seite 76](#) beschrieben über mehrere Wege erfolgen, ist aber immer paßwortgesichert. Jeder Fehlversuch wird mit Angabe der Quelle per Syslog-Message protokolliert und erzeugt einen entsprechenden SNMP-Trap. Nach mehreren Fehlversuchen werden Pausen eingeführt, um ein automatisiertes Ausprobieren zu erschweren.

**Achtung!**

Alle BinTec-Router werden mit gleichen Benutzernamen und Paßwörtern ausgeliefert. Sie sind daher nicht gegen einen unauthorisierten Zugriff geschützt, solange die Paßwörter nicht geändert wurden. Die Vorgehensweise bei der Änderung von Paßwörtern ist unter "[Paßwortänderung](#)", [Seite 85](#) beschrieben.

- Ändern sie unbedingt die Paßwörter wie in [Kapitel 4.2, Seite 76](#) beschrieben.
- Achten Sie zusätzlich darauf, daß Unbefugte nicht auf die Stromzufuhr zu **X4000**, 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 **X4000** 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 14.1, Seite 428](#)).



Wenn Sie ein Software-Update durchführen (siehe [Kapitel 11.2, Seite 388](#)), sollten Sie den Autologout ausschalten: Geben Sie `t 0` in die SNMP-Shell ein.



Es ist möglich, zusätzliche Benutzeraccounts mit Hilfe von SNMP-Kommandos anzulegen (siehe [Software Reference](#)). Einem Benutzer kann dabei ein bestimmtes Paßwort und eine bestimmte Aktion zugeordnet werden.

10.2.2 Überprüfen der eingehenden Rufnummer

CLID

Mit Hilfe von Calling Line Identification (➤➤ **CLID**) überprüft **X4000** 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 **X4000** anhand des Screening-Indikators in der Setup-Nachricht des ISDN-**➤➤ D-Kanals** erkennen. Für den Screening-Indikator gibt es vier Werte:

- *user*: Die Angabe der Calling Party's Number stammt von der Gegenseite und wurde vom Netz nicht überprüft.
- *user_verified*: Die Calling Party's Number wurde von der Vermittlungsstelle geprüft und ist richtig.
- *user_failed*: Die Calling Party's Number wurde von der Vermittlungsstelle geprüft und ist falsch.
- *network*: Die Angabe der Calling Party's Number stammt direkt von der Vermittlungsstelle (Normalfall).

Wenn **X4000** bei eingehenden Rufen den Screen-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**.

10.2.3 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 7.3, Seite 162](#) und [Kapitel 8.1.3, Seite 200](#).

10.2.4 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. **X4000** 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 10-7: **WAN PARTNER** ➤ **EDIT** ➤ **ADVANCED SETTINGS**

Callback enthält folgende Auswahlmöglichkeiten:

Mögliche Werte	Bedeutung
<i>no</i>	X4000 führt keinen Rückruf aus.
<i>expected (awaiting callback)</i>	X4000 ruft den WAN-Partner an, um den Call-back zu initiieren.
<i>yes (PPP negotiation)</i>	X4000 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.
<i>yes (delayed, CLID only)</i>	X4000 ruft nach ca. vier Sekunden zurück, wenn Ihr Router vom WAN-Partner dazu aufgefordert wird.
<i>yes (PPP negotiaton, callback optional)</i>	Entspricht dem Wert <i>yes (PPP negotiation)</i> , beinhaltet allerdings eine Abbruchoption. Der Microsoft-Client hat hier die Möglichkeit, den Callback abubrechen und die initiale Verbindung zu X4000 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 X4000 eingetragen ist, kann diese Abbruchoption nicht genutzt werden!
<i>yes</i>	X4000 ruft sofort zurück, wenn Ihr Router vom WAN-Partner dazu aufgefordert wird.

Tabelle 10-8: **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 **Callback** aus.
- Bestätigen Sie mit **OK**.

10.2.5 Closed User Group

X4000 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 den CUG-Index ein.
- Bestätigen Sie mit **OK**.

10.2.6 Zugriff auf Remote-CAPI

Zu den Besonderheiten der BinTec-Router gehört die Implementierung der Programmierschnittstellen ➤➤ **Remote-CAPI** und Remote-TAPI (nur bei PABX-Geräten). Dadurch können Applikationen auf Rechnern im LAN die 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 authentifizierte Benutzer auf die Remote-CAPI-Schnittstelle von **X4000** zugreifen können (siehe [Kapitel 7-3, Seite 144](#)).

Filter Mit der Definition von Filtern (siehe [Kapitel 10.2.8, Seite 349](#)) und lokalen Filtern (siehe [Kapitel 10.2.9, Seite 363](#)) können Sie unbefugten Zugriff ebenfalls verhindern.

10.2.7 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.

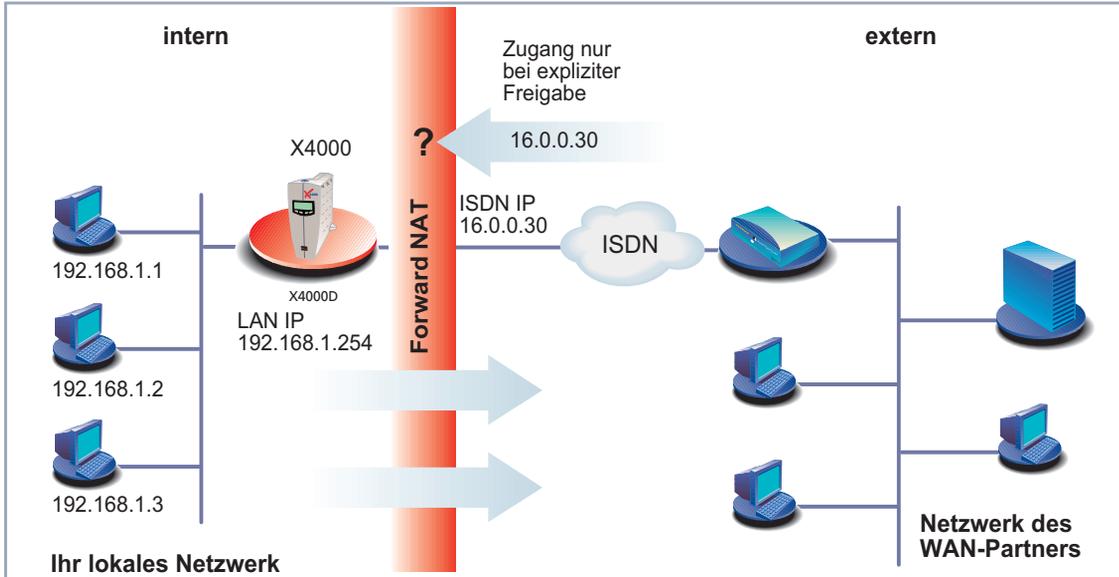


Bild 10-1: Forward NAT

- Permanente Überwachung der Verbindungen über den Router mit Quell- und Zielangabe der Adressen und ➤➤ **Ports**. Beachten Sie hierzu Ihre Syslog-Messages!

NAT bezieht sich immer auf eine Schnittstelle. **X4000s** 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 **X4000** mit einer Statusanzeige für aktuelle NAT-Einstellungen aufgelistet:

Feld	Bedeutung
Name	Name der Schnittstelle
Nat	Zeigt an, ob NAT für die entsprechende Schnittstelle aktiviert ist. Mögliche Werte: <ul style="list-style-type: none"> ■ <i>off</i>: Kein NAT aktiviert. ■ <i>on</i>: Forward NAT aktiviert. ■ <i>reverse</i>: 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 10-9: **IP ➤ NETWORK ADDRESS TRANSLATION**

In **IP** ► **NETWORK ADDRESS TRANSLATION** ► **EDIT** aktivieren Sie NAT für eine Schnittstelle von **X4000**:

Feld	Bedeutung
Network Address Translation	Definiert die Art von NAT für die ausgewählte Schnittstelle. Mögliche Werte: <ul style="list-style-type: none">■ <i>off</i>: Kein NAT ausführen.■ <i>on</i>: Forward NAT ausführen.■ <i>reverse</i>: Reverse NAT ausführen.

Tabelle 10-10: **IP** ► **NETWORK ADDRESS TRANSLATION** ► **Eingabetaste**

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	<p>Dienst, der für Verbindungen zum unter Destination definierten Host erlaubt wird. Mögliche Werte:</p> <ul style="list-style-type: none"> ■ <i>ftp</i> ■ <i>telnet</i> ■ <i>smtp</i> ■ <i>domain/udp</i> ■ <i>domain/tcp</i> ■ <i>http</i> ■ <i>nntp</i> ■ <i>user defined</i>: Wenn Sie keinen der vordefinierten Dienste verwenden. Geben Sie unter Protocol und Port die erforderlichen Werte ein, um einen Dienst zu definieren.
Protocol	<p>Nur bei Service = <i>user defined</i>. Definiert das erlaubte Protokoll. Mögliche Werte:</p> <ul style="list-style-type: none"> ■ <i>icmp</i> ■ <i>tcp</i> ■ <i>udp</i> ■ <i>gre</i> ■ <i>esp</i> ■ <i>ah</i> ■ <i>l2tp</i>

Feld	Bedeutung
Port (-1 for any)	Nur bei Service = <i>user defined</i> . 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 10-11: **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**.



Sobald Sie hier einen Eintrag mit **SAVE** bestätigen, wird dieser sofort wirksam. Denken Sie immer daran, insbesondere wenn Sie NAT von einem Remote-Host konfigurieren, z. B. mit telnet!

Gehen Sie folgendermaßen vor, um 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 **Protocol** aus.
- Geben Sie gegebenenfalls **Port (-1 for any)** ein.
- Geben Sie **Destination** ein.
- Bestätigen Sie mit **SAVE**.

- Wiederholen Sie diese Schritte, um mehrere Freigaben für die ausgewählte NAT-Schnittstelle zu definieren.

10.2.8 Filter (Access Lists)

IP-Filter (➤➤ **Access Lists**) auf **X4000** basieren auf einem Konzept von ➤➤ **Filtern**, Regeln und sogenannten Ketten. IP-Filter reagieren auf eingehende Datenpakete, sie können also bestimmten Daten den Zutritt zu **X4000** 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 Zielport. Wenn Sie also ein Filter definieren, teilen Sie **X4000** mit: "Achte auf diejenigen Datenpakete, auf die folgendes zutrifft: ...".

Regel Mit einer Regel teilen Sie **X4000** mit, wie er mit den ausgefilterten Datenpaketen umgehen soll – ob er sie durchlassen oder abweisen soll. Sie können auch mehrere Regeln definieren, die Sie in Form einer Kette organisieren und ihnen damit eine bestimmte Reihenfolge geben.

Kette 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 jeder **X4000**-Schnittstelle individuell eine Regelkette festlegen.

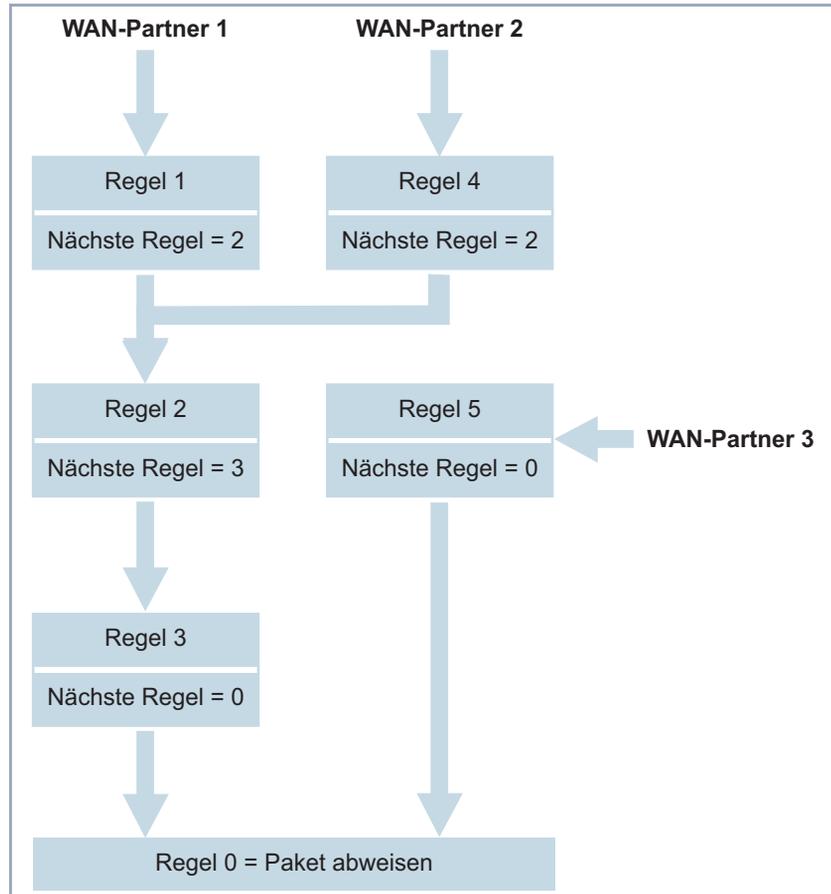


Bild 10-2: Regelketten für unterschiedliche Schnittstellen

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. X4000 vergibt hier neu definierten Filtern automatisch eine Nummer.
Protocol	Legt ein Protokoll fest. Mögliche Werte: <i>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.</i> <i>any</i> paßt auf jedes Protokoll, <i>tcp</i> paßt nur auf TCP-Datenpakete, usw.
Type	Nur bei Protocol = <i>icmp</i> . Mögliche Werte: <i>any, echo reply, destination unreachable, source quench, redirect, echo, time exceeded, param problem, timestamp, timestamp reply, address mask, address mask reply</i> . Siehe RFC 792.
Connection State	Bei Protocol = <i>tcp</i> können Sie ein Filter definieren, das auf dem Status der TCP-Verbindung basiert. Mögliche Werte: <ul style="list-style-type: none"> ■ <i>established</i>: Das Filter paßt auf diejenigen TCP-Pakete, die beim Routing über X4000 keine neue TCP-Verbindung öffnen würden. ■ <i>any</i>: Das Filter paßt auf alle TCP-Pakete.
Source Address	Quell-IP-Adresse der Datenpakete, auf die das Filter paßt.

Feld	Bedeutung
Source Mask	Quell-Netzmaske. 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. <i>specify range</i> : 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 Ziell-Port-Nummern, auf den das Filter paßt.
Type of Service (TOS)	Type of Service
TOS Mask	Maske für Type of Service

Tabelle 10-12: IP ► ACCESS LISTS ► FILTER

Die Felder **Source Port** bzw. **Destination Port** enthalten folgende Auswahlmöglichkeiten:

Mögliche Werte	Bedeutung
<i>any</i>	Das Filter paßt auf alle >> Port -Nummern.
<i>specify</i>	Ermöglicht Eingabe einer Port-Nummer unter Specify Port .
<i>specify range</i>	Ermöglicht Eingabe eines Bereiches von Port-Nummern unter Specify Port .
<i>priv (0..1023)</i>	Port-Nummern: 0 ... 1023.
<i>server (5000..32767)</i>	Port-Nummern: 5000 ... 32767.
<i>clients 1 (1024..4999)</i>	Port-Nummern: 1024 ... 4999.
<i>clients 2 (32768..65535)</i>	Port-Nummern: 32768 ... 65535.
<i>unpriv (1024..65535)</i>	Port-Nummern: 1024 ... 65535.

Tabelle 10-13: **Source Port** bzw. **Destination Port**

Port-Nummern Port-Nummern sind wie folgt verteilt:

0 ... 1023	1024 ... 4999	5000 ... 32767	32768 ... 65535
Well Known Ports, d. h. fest vergeben: <i>priv (0..1023)</i>	Die Ports werden von >> Clients bzw. >> Servern dynamisch angelegt und haben keine feste Bedeutung (mit Ausnahme von besonderen Vereinbarungen): <i>unpriv (1024..65535)</i>		
	<i>clients 1 (1024..4999)</i>	<i>server (5000..32767)</i>	<i>clients 2 (32768..65535)</i>

Tabelle 10-14: Bereiche von Portnummern

Im Folgenden eine Übersicht über einige häufig gebrauchte Port-Nummern mit den zugewiesenen Diensten:

Dienst	Protokoll	Port-Nummer
File Transfer Protocol (➤➤ FTP) (Daten)	TCP	20
File Transfer Protocol (FTP) (Kommandos)	TCP	21
Telnet	TCP	23
Simple Mail Transfer Protocol (SMTP)	TCP	25
Domain Name Server (➤➤ DNS)	TCP, UDP	53
Trivial File Transfer Protocol (➤➤ TFTP)	UDP	69
HTTP	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 10-15: 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:

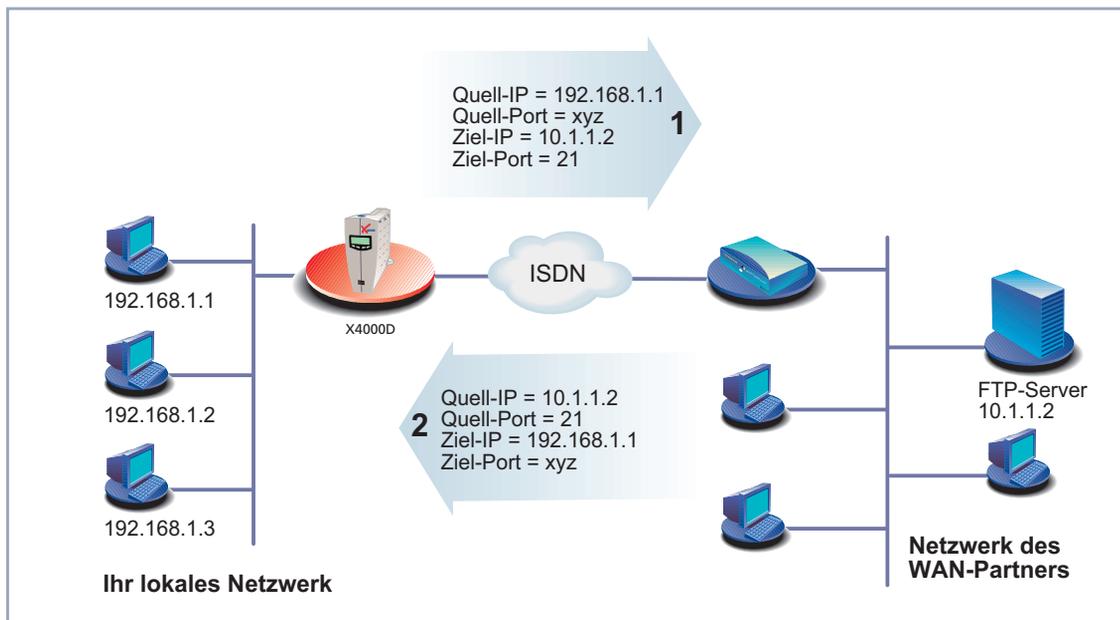


Bild 10-3: Beispiel: FTP-Verbindung

In **IP** ► **ACCESS LISTS** ► **RULES** definieren Sie Regeln:

Feld	Bedeutung
Index	Kann nicht verändert werden. X4000 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 <i>none</i> beginnen Sie eine neue eigenständige Kette.
Action	Legt fest, wie mit einem ausgefilterten Datenpaket verfahren wird.
Filter	Filter, das verwendet wird.
Next Rule	Erscheint nur, wenn eine bestehende Regel editiert wird. Legt fest, welche Regel als nächste angewendet wird.

Tabelle 10-16: **IP** ► **ACCESS LISTS** ► **RULES**

Das Feld **Action** enthält folgende Auswahlmöglichkeiten:

Mögliche Werte	Bedeutung
<i>allow M</i>	Paket durchlassen, wenn das Filter paßt.
<i>allow !M</i>	Paket durchlassen, wenn das Filter nicht paßt.
<i>deny M</i>	Paket abweisen, wenn das Filter paßt.
<i>deny !M</i>	Paket abweisen, wenn das Filter nicht paßt.
<i>ignore</i>	Nächste Regel anwenden.

Tabelle 10-17: **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 10-18: **IP** ► **ACCESS LISTS** ► **RULES** ► **REORG**

Wenn Sie so eine Kette neu organisieren, nummeriert **X4000** nach Auswahl von **Index of Rule that gets Index 1** die verbleibenden Regeln neu:

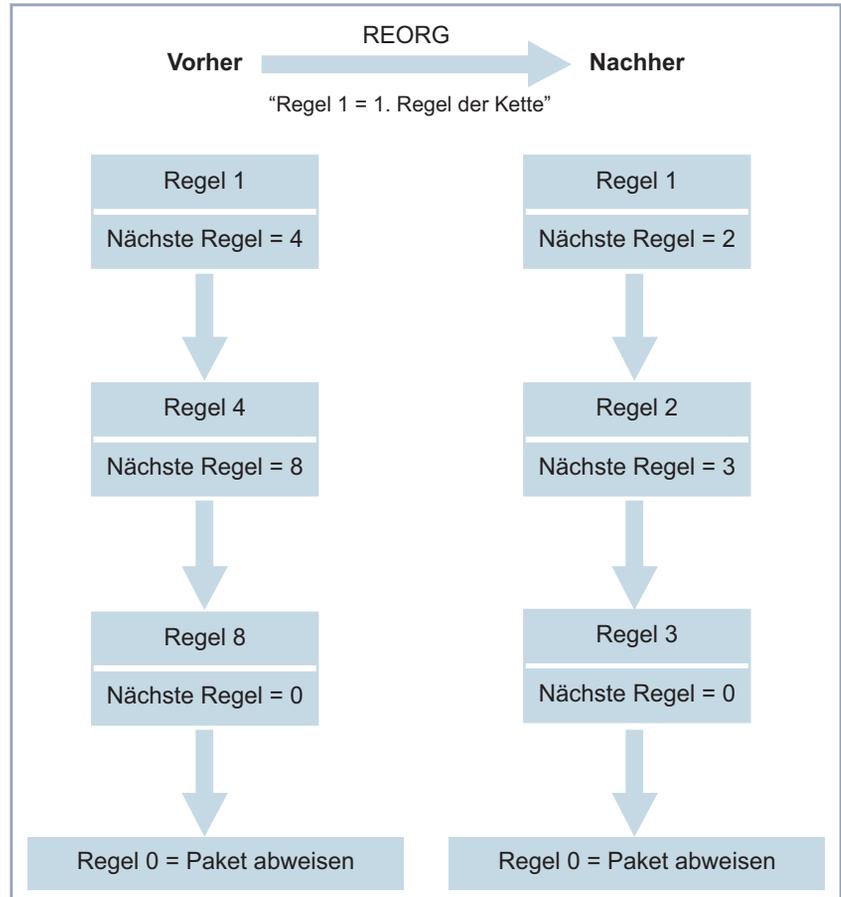


Bild 10-4: Beispiel für die Neuorganisation einer Kette

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 **X4000** abgewiesen wird:



Standardmäßig wird immer die Regel mit **Index = 1** für eine neuerstellte Schnittstelle (z. B. zu einem WAN-Partner) als erste Regel angewendet.

Feld	Bedeutung
Interface	X4000 -Schnittstelle
First Rule	Legt fest, welche Regel als erste für Datenpakete, die über Interface X4000 erreichen, angewendet wird. Mit <i>none</i> 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: <ul style="list-style-type: none"> ■ <i>no</i>: Paket wird abgewiesen, Absender wird mit einer ICMP-Fehlermeldung darüber informiert. ■ <i>yes</i>: 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: <ul style="list-style-type: none"> ■ <i>none</i>: Keine Syslog-Meldung. ■ <i>info</i>: Eine Syslog-Meldung mit Angabe von Protokollnummer, Quell-IP-Adresse und Quell-Port-Nummer wird generiert. ■ <i>dump</i>: Eine Syslog-Meldung mit dem Inhalt der ersten 64 Bytes des abgewiesenen Pakets wird generiert.

Tabelle 10-19: **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 "ausperren". Wenn Sie z. B. das erste Filter mit einer Regel verknüpfen, die **Action = Allow M** ausführt, kommt wirklich nur durch, was Sie mit dem Filter ausdrücklich erlaubt haben. So kann es leicht passieren, daß Ihr Zugriff auf **X4000** 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 **X4000** zugreifen.
- Wenn Sie über die serielle Schnittstelle oder ISDN-Login auf **X4000** zugreifen, passiert Ihnen zumindest während der Konfiguration nichts.

- Filter**
- Gehen Sie zu **IP** ➤ **ACCESS LISTS** ➤ **FILTERS**.
 - Fügen Sie mit **ADD** einen neuen Eintrag hinzu oder wählen Sie einen bestehenden Eintrag aus und bestätigen mit der **Eingabetaste**, um ihn zu verändern.
 - Geben Sie **Description** ein.
 - Wählen Sie **Protocol** aus.
 - Geben Sie gegebenenfalls **Source Address** ein.
 - Geben Sie gegebenenfalls **Source Mask** ein.
 - Wählen Sie **Source Port** aus.
 - Geben Sie gegebenenfalls **Specify Port** ein.
 - Geben Sie gegebenenfalls **Destination Address** ein.
 - Geben Sie gegebenenfalls **Destination Mask** ein.
 - Wählen Sie **Destination Port** aus.
 - Geben Sie gegebenenfalls **Specify Port** ein.
 - Bestätigen Sie mit **SAVE**.
 - Wiederholen Sie diese Schritte so oft, bis Sie alle gewünschten Filter definiert haben.



Vergessen Sie nicht, gegebenenfalls ein Filter für die Freigabe der restlichen Datenpakete zu definieren (**Protocol = any, Source Port = any, Destination Port = any**).

➤ Verlassen Sie **IP** ➤ **ACCESS LISTS** ➤ **FILTERS** mit **EXIT**.

Regeln

- Gehen Sie zu **IP** ➤ **ACCESS LISTS** ➤ **RULES**, um die Filter 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 **Action** aus.
- Wählen Sie **Filter** aus.
- Wählen Sie **Next Rule** aus, wenn Sie eine bestehende Regel verändern.
- Bestätigen Sie mit **SAVE**.
- Wiederholen Sie diese Schritte so oft, bis Sie alle gewünschten Regeln definiert haben.



Vergessen Sie nicht, gegebenenfalls als letzte Regel in der Kette eine Regel 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 7.1.5, Seite 132](#) Schritt für Schritt erläutert.

10.2.9 Lokale Filter

Der Zugang zu den lokalen UDP- bzw. TCP-Diensten auf **X4000** (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 10.2.7, Seite 344](#)) oder globalen Filtern (siehe [Kapitel 10.2.8, Seite 349](#)) verboten wurde.

Strategie

Sobald auf **X4000** mindestens ein Eintrag für lokale Filter besteht, werden eingehende Anfragen auf die entsprechenden lokalen Dienste von **X4000** nur erlaubt, wenn

1. die Quell-Adresse 127.0.0.1 ist (Loopback-Adresse), oder
2. kein Eintrag für den entsprechenden Dienst vorhanden ist, oder

3. der eingehende Ruf ausdrücklich durch mindestens einen Eintrag erlaubt wird.

Dabei werden die vorhandenen Einträge in der Reihenfolge abgearbeitet, wie 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 Performance beim normalen Routing nicht beeinträchtigt.

Die Konfiguration erfolgt in **IP ► LOCAL SERVICES ACCESS CONTROL ► ADD:**

Feld	Bedeutung
Service	<p>Definiert den lokalen Dienst auf X4000, zu dem der Zugang u. a. mit diesem Eintrag geregelt werden soll. Mögliche Werte:</p> <ul style="list-style-type: none"> <input type="checkbox"/> <i>snmp(udp)</i> <input type="checkbox"/> <i>rip (udp)</i> <input type="checkbox"/> <i>bootps(udp)</i> <input type="checkbox"/> <i>dns(udp)</i> <input type="checkbox"/> <i>telnet(tcp)</i> <input type="checkbox"/> <i>trace(tcp)</i> <input type="checkbox"/> <i>snmp(tcp)</i> <input type="checkbox"/> <i>capi(tcp)</i> <input type="checkbox"/> <i>tapi(tcp)</i> <input type="checkbox"/> <i>rfc1086(tcp)</i> <input type="checkbox"/> <i>http(tcp)</i> <input type="checkbox"/> <i>nbns(udp)</i> <input type="checkbox"/> <i>statmon(udp)</i>
Verify IP Address	<p>Definiert, ob bei einem eingehenden Ruf auf den unter Service festgelegten Dienst die Quell-IP-Adresse überprüft werden soll. Mögliche Werte:</p> <ul style="list-style-type: none"> <input type="checkbox"/> <i>verify</i> <input type="checkbox"/> <i>don't verify</i>

Feld	Bedeutung
IP Address	(nur bei Verify IP Address = verify) Definiert eine IP-Adresse bzw. Netzwerk- adresse (zusammen mit Mask), von der einge- hende Anfragen auf den unter Service festgelegten Dienst erlaubt werden. Hat eine Anfrage eine andere Quell-Adresse, 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 wer- den. Hat eine Anfrage eine andere Quell- Adresse, wird zum nächsten Eintrag überge- gangen. Ist der Wert von Mask <i>0.0.0.0</i> oder <i>255.255.255.255</i> , 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 über- prüft werden soll, über welche X4000 -Schnitt- stelle der Ruf eingeht. Mögliche Werte: ■ <i>verify</i> ■ <i>don't verify</i>
Interface	(nur bei Verify Interface = verify) Definiert eine Schnittstelle von X4000 . Erreicht X4000 ein eingehender Ruf auf den unter Service festgelegten Dienst über diese Schnitt- stelle, wird die Verbindung erlaubt. Überquert der eingehende Ruf eine andere Schnittstelle, wird zum nächsten Eintrag übergegangen.

Tabelle 10-20: **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 **X4000** ihn 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 **Service** aus.
- Wählen Sie **Verify IP Address** aus, z. B. *verify*.
- Geben Sie gegebenenfalls **IP Address** ein.
- Geben Sie gegebenenfalls **Mask** ein.
- Wählen Sie **Verify Interface** aus, z. B. *verify*.
- Wählen Sie gegebenenfalls **Interface** aus.
- Bestätigen Sie mit **SAVE**. Der Eintrag wird aufgelistet.

10.2.10 Backroute Verification

Hinter diesem Begriff versteckt sich eine einfache, aber sehr leistungsfähige Funktion von **X4000**. 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 unbekanntete 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**.

10.2.11 TAF-Client

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 **X4000** können Sie diese Funktion freischalten (mit Zusatzlizenz) und den Router als TAF-Server bzw. TAF-Client einrichten. Die genaue Darstellung der Funktionsweise und die erforderlichen Konfigurationsschritte finden Sie in [BRICKware for Windows](#).

10.2.12 Extended IP-Routing (XIPR)

Ergänzend zu der normalen Routing-Tabelle kann **X4000** auch Routing-Entscheidungen aufgrund einer zusätzlichen Tabelle, der Extended Routing-Tabelle, treffen (Erweitertes IP-Routing). Dabei kann **X4000** neben der 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* bzw. in der MIB-Tabelle **ipExtRtTable**.

Eine ausführliche Beschreibung (einschließlich der Konfiguration anhand der MIB-Variablen) finden Sie in der [Software Reference](#), zur Konfiguration mit dem Setup Tool beachten Sie bitte die entsprechenden Ergänzungen in der nächsten Version des Benutzerhandbuchs.

10.3 Abhörsicherung

Für sicherheitskritische PPP-Verbindungen auf sicherheitskritischen Verbindungen können Sie einen Verschlüsselungsmechanismus einsetzen, wenn beide Verbindungspartner diesen unterstützen. Folgende Funktionen sind möglich:

- Verschlüsselung ([Kapitel 10.3.1, Seite 370](#))
- VPN (mit Zusatzlizenz) ([Kapitel 10.3.2, Seite 373](#))

10.3.1 Verschlüsselung

X4000 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 **X4000** 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 **X4000** 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 **X4000** eine Lizenz für VPN eingetragen ist.

Die Konfiguration erfolgt in

■ **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	<p>Legt die Art der Verschlüsselung fest. Mögliche Werte:</p> <ul style="list-style-type: none"> ■ MPPE 40: MPPE Version 1 mit 40-Bit-Schlüssel ■ MPPE 56: MPPE Version 1 mit 56-Bit-Schlüssel ■ MPPE V2 40: MPPE Version 2 mit 40-Bit-Schlüssel ■ MPPE V2 56: MPPE Version 2 mit 56-Bit-Schlüssel ■ DES 56: DES mit 56-Bit-Schlüssel ■ Blowfish 56: Blowfish mit 56-Bit-Schlüssel ■ none: keine Verschlüsselung <p>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.</p>

Tabelle 10-21: **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: ■ <i>authentication</i> (Standardwert): Schlüssel wird von X4000 automatisch generiert. ■ <i>static</i> : 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 10-22: **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**.

10.3.2 VPN (mit Zusatzlizenz)

Mit Hilfe von PPTP (Point to Point Tunneling Protocol) kann **X4000** ein VPN (Virtual Private Network) herstellen. Dies dient zu einer sicheren (verschlüsselten) Übertragung von Daten über WAN-Verbindungen, z. B. über das Internet. So kann z. B. von Außendienstmitarbeitern per Laptop ein Zugang auf Daten des Firmennetzes kostengünstig über das Internet realisiert werden (Einwahl über einen örtlichen Internet Service Provider).



Detaillierte Informationen und Konfigurationshinweise (mit Beispielen) finden Sie in der [Extended Features Reference](#).

10.4 Besonderheiten

Folgende Besonderheiten unterstützen die Sicherheit Ihres Netzwerks:

- Startup-Verhalten ([Kapitel 10.4.1, Seite 374](#))
- Auto-Logout ([Kapitel 10.4.2, Seite 374](#))
- Vorbeugung gegen Denial-of-Service-Attacken ([Kapitel 10.4.3, Seite 374](#))

10.4.1 Startup-Verhalten

X4000 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.

10.4.2 Auto-Logout

Verbindungen zu **X4000** über telnet, **isdnlogin** oder seriell werden automatisch getrennt, wenn 15 Minuten lang keine Eingabe über die Tastatur erfolgt. Damit wird das Auslesen oder Ändern der Systemkonfiguration auf "vergessenen" Verbindungen erschwert. Den Zeitraum können Sie mit dem Kommando `t <Zeit in Sekunden>` verändern (siehe [Kapitel 14.1, Seite 428](#)).

10.4.3 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.

Z. B. existiert an allen **X4000**-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 10.2.10](#), [Seite 367](#)).

DoS-Angriffe, die auf Systemstörung durch Überlaufen von Logdateien (Syslog-Messages) spekulieren, können Sie durch geeignete Platzierung und Größenlimitierung dieser Dateien begegnen.

10.5 Checkliste

Die nachfolgende Liste gibt die wichtigsten sicherheitskritischen Punkte an, die Sie bei der Konfiguration von **X4000** beachten sollten:

- Haben Sie alle vier Paßwörter für den Systemzugang (admin, read, write, http) verändert? Siehe [Kapitel 4.2, Seite 76](#).
- Werden die Aktivitäten von **X4000** auf mindestens einem externen Rechner ausreichend genau protokolliert und überprüfen Sie die Syslog-Messages regelmäßig? Siehe [Kapitel 10.1.1, Seite 320](#).
- Haben Sie den Zugriff auf die lokalen Dienste und Ressourcen eingeschränkt auf bekannte Rechner oder Netze? Insbesondere die Zugänge per CAPI, SNMP, HTTP, Trace und Telnet sollten Sie nur bekannten Rechnern gestatten.
- Liegen per TFTP abgespeicherte Konfigurationsdateien an einem sicheren Ort?
- Haben Sie alle PPP-Zugänge mit Paßwort gesichert?
- Haben Sie ggf. für die Verbindung zum Internet Service Provider (ISP) Network Address Translation (NAT) aktiviert? Siehe [Kapitel 10.2.7, Seite 344](#).
- 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 10.2.8, Seite 349](#).
- Haben Sie ggf. den Zugang über ISDN-Login für Fernwartung gesperrt? Haben Sie einen geeigneten Eintrag unter **CM1BRI, ISDN SO** ► **INCOMING CALL ANSWERING** gemacht? Siehe ["Incoming Call Answering", Seite 142](#).

Als zusätzliche Punkte sollten Sie beachten:

- Verwenden Sie für PPP-Verbindungen Callback nach dem Microsoft-Verfahren? Beachten Sie bitte die Hinweise in [Kapitel 10.2.4, Seite 341](#).
- Setzen Sie auf sicherheitskritischen Verbindungen ein Verschlüsselungsprotokoll zur Abhörsicherung ein? Siehe [Kapitel 10.3.1, Seite 370](#).

- 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 8.2.8, Seite 236](#).
- 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 7-3, Seite 144](#))?
- Sind eventuell zusätzlich angelegte Benutzeraccounts unproblematisch?
- Haben Sie das Abhören von Verbindungen auf dem Ethernet durch eine geeignete LAN-Infrastruktur verhindert?

11 Konfigurationsmanagement

In diesem Kapitel finden Sie Hinweise zum Verwalten Ihrer Konfigurationsdateien und zum Updaten der Software von **X4000**. Es umfasst folgende Bereiche:

- Verwalten der Konfigurationsdateien:
 - Wo sind die Konfigurationsdateien?
 - Was ist Flash und Memory?
 - Wie kann ich mit Konfigurationsdateien umgehen?
- Software-Update durchführen
 - Wie bleibe ich immer auf dem neuesten Stand?
 - Wie lade ich ein neues Boot-Image?

11.1 Konfigurationsdateien verwalten

- Flash** **X4000** liest seine Konfigurationsinformationen aus Konfigurationsdateien. Diese Konfigurationsdateien sind gespeichert im Flash EEPROM (electronically erasable programmable read-only memory) von **X4000**. Im Flash-Speicher können einige verschiedene Konfigurationsdateien gespeichert werden. Auch wenn **X4000** 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 **X4000** einstellen. Der Inhalt von Memory geht verloren, wenn **X4000** ausgeschaltet wird. Wenn Sie Ihre Konfiguration ändern und diese Änderungen auch beim nächsten Start von **X4000** beibehalten wollen, müssen Sie die geänderte Konfiguration vor dem Ausschalten im Flash speichern: **Exit** ► **Save as boot configuration and exit** (siehe [Kapitel 7.4, Seite 191](#)). Diese Datei wird damit als Boot-Konfigurationsdatei mit dem Namen "boot" im Flash gespeichert. Beim Starten von **X4000** wird dann genau diese Datei, also die Konfigurationsdatei mit dem Namen "boot", im Memory geladen und damit wirksam.
- Aktionen** Stellen Sie sich den Flash-Speicher als Verzeichnis von Konfigurationsdateien vor. Die Dateien in diesem Verzeichnis können kopiert, verschoben, gelöscht und neu angelegt werden. Es ist auch möglich, Konfigurationsdateien zwischen **X4000** 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 **X4000** auf Ihrem lokalen Rechner abspeichern.



Die mit dem TFTP-Server der DIME Tools zu transferierenden Dateien dürfen maximal aus 8 Zeichen bestehen (+ maximal 3 Zeichen als Anhang), z. B. b5104.x4a.

- Unix** Unter Unix ist ein TFTP-Server Teil des Systems, beachten Sie bitte die Hinweise in der Software Reference.

Mit Hilfe des Setup Tools können Sie die verschiedenen Aktionen ausführen:

- Gehen Sie in das Menü **CONFIGURATION MANAGEMENT**.

X4000 Setup Tool [CONFIG]:Configuration Management	BinTec Communications AG 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 Hostname (falls der Hostname aufgelöst werden kann) des TFTP-Servers von bzw. zu dem Sie eine Konfigurationsdatei transferieren wollen.
TFTP File Name	Name der Konfigurationsdatei auf dem TFTP-Server (ohne Pfadangabe).
Name in Flash	Name der Konfigurationsdatei im Flash.
New Name in Flash	Name der neu zu erzeugenden Konfigurationsdatei im Flash (bei Operation = <i>move</i> oder <i>copy</i>).
Type of last operation	Vorhergehende Aktion (seit dem letzten X4000 -Start).
State of last operation	Status der letzten Aktion.

Tabelle 11-1: **CONFIGURATION MANAGEMENT**

Das Feld **Operation** enthält folgende Auswahlmöglichkeiten:

Mögliche Werte	Bedeutung
<i>save</i> (MEMORY --> FLASH)	Alle aktuellen Einstellungen von Memory ins Flash als Konfigurationsdatei <Name in Flash> speichern. <Name in Flash> wird dabei überschrieben bzw. neu erzeugt.
<i>load</i> (FLASH --> MEMORY)	Konfigurationsdatei <Name in Flash> vom Flash ins Memory laden. Die Einstellungen von <Name in Flash> werden sofort wirksam.
<i>move</i> (FLASH --> FLASH)	Konfigurationsdatei <Name in Flash> in <New Name in Flash> umbenennen.
<i>copy</i> (FLASH --> FLASH)	Konfigurationsdatei <Name in Flash> als <New Name in Flash> kopieren.
<i>delete</i> (FLASH)	Konfigurationsdatei <Name in Flash> löschen.
<i>put</i> (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.
<i>get</i> (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 X4000 wirksam werden.

Mögliche Werte	Bedeutung
<i>state</i> (<i>MEMORY</i> --> <i>TFTP</i>)	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.
<i>reboot</i>	X4000 neu starten. Einstellungen im Memory gehen werden durch Einstellungen von boot aus Flash ersetzt.

Tabelle 11-2: **Operation**

Das Feld **State of last operation** kann folgendes anzeigen:

Mögliche Werte	Bedeutung
<i>todo</i>	Die Aktion wurde noch nicht gestartet.
<i>running</i>	Die Aktion wird gerade ausgeführt.
<i>done</i>	Die Aktion wurde erfolgreich ausgeführt.
<i>error</i>	Die Aktion konnte nicht vollständig ausgeführt werden (siehe Syslog-Message).

Tabelle 11-3: **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 **X4000s** Boot-Datei gelöscht, **X4000** kann beim Hochfahren keine Konfiguration mehr laden. Benennen Sie gegebenenfalls die zu transferierende Datei um!



Für Ausführen von *put* (Flash --> TFTP), *get* (TFTP --> Flash) und *state* (MEMORY --> TFTP) benötigen Sie einen TFTP-Server auf dem Host, zu oder von dem Sie eine Konfigurationsdatei transferieren wollen.

Wenn der TFTP-Host ein Windows-PC ist, klicken Sie auf **Programme** ► **BRICKware** ► **DIME Tools** im Windows-Startmenü, um die **DIME Tools** zu öffnen und aktivieren Sie den TFTP-Server mit **File** ► **TFTP Server**, bevor Sie die entsprechende Aktion durchführen.



Wenn Sie Ihren Windows-PC als TFTP-Host nutzen wollen, aber nicht sicher sind, wie die IP-Adresse des PCs lautet, gehen Sie folgendermaßen vor:

Windows 95:

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

Es erscheint ein Fenster, in dem Sie die IP-Adresse Ihres Rechner und andere Netzinformationen sehen.

Windows NT:

- Klicken Sie im Windows-Startmenü auf **Programme** ► **Eingabeaufforderung**.
- Geben Sie `ipconfig` oder `ipconfig/all` ein, um Ihre IP-Adresse Ihres Rechners und andere Netzinformationen abzufragen.

Aktion ausführen Gehen Sie folgendermaßen vor, um eine Aktion auszuführen:

- Wählen Sie **Operation** aus.
- Aktivieren Sie einen TFTP-Server, falls Sie als **Operation** *put*, *get* oder *state* ausgewählt haben.
- Wählen Sie in **CONFIGURATION MANAGEMENT** die erforderlichen Einstellungen aus bzw. tragen Sie die erforderlichen Werte ein.
- Wählen Sie **START OPERATION** aus und bestätigen Sie mit der **Eingabetaste**.

Solange die Aktion ausgeführt wird, erscheint in der Hilfszeile des Setup Tool **OPERATING**, **State of last operation** zeigt *running* an.

Wenn die Aktion erfolgreich ausgeführt wurde, wird sie unter **Type of last operation** angezeigt, **State of last operation** nimmt den Wert *done* an.



Wenn unter **State of last operation error** angezeigt wird, überprüfen Sie Ihre Einstellungen:

- Haben Sie unter TFTP Server IP Address eine falsche IP-Adresse angegeben?
- Besteht der Name der Konfigurationsdatei aus mehr als 8 Zeichen und die Extension aus mehr als 3 Zeichen (bei Verwendung der DIME Tools)?
- Unterstützt der Host nicht TFTP (haben Sie vergessen, vor Ausführen der Aktion den TFTP-Server der DIME Tools zu starten)?
- Liegt die Quelldatei nicht im konfigurierten Verzeichnis des TFTP-Pfades der DIME Tools (Bei **Operation = get**)? Beachten Sie [BRICKware for Windows](#), um den TFTP-Pfad zu verändern.
- Wenn diese Punkte nicht zutreffen, gehen Sie folgendermaßen vor, um die Fehlerursache zu finden:
 - Verlassen Sie das Setup Tool.
 - Geben Sie in der SNMP-Shell ein: `debug config &`.
 - Öffnen Sie erneut das Setup Tool mit `setup`.
 - Führen Sie die gewünschte Aktion in **CONFIGURATION MANAGEMENT** aus. In der Hilfszeile des Setup Tool Menüs wird bei Auftreten eines Fehlers eine Fehlermeldung mit der Ursache angezeigt.
 - Beseitigen Sie die Ursache des Problems und führen Sie die Aktion erneut aus.
- Verlassen Sie **CONFIGURATION MANAGEMENT** mit **EXIT**.

Beispiel Sie haben die Konfigurationsdatei `brick.cf` erstellt, z. B. mit Hilfe des Configuration Wizard. Sie haben die Datei nicht über die serielle Schnittstelle auf **X4000** 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 **X4000** 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 **X4000** gespeichert.

Gehen Sie anschließend folgendermaßen vor, um die Einstellungen von *brick.cf* sofort auf **X4000** 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 **X4000** 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.

11.2 Software-Update durchführen

Da BinTec Communications AG die Software für alle Produkte ständig weiterentwickelt und Sie sicher die neuen Funktionen von **X4000** nutzen wollen, erfahren Sie hier, wie Sie ein Software-Update durchführen können.

www.bintec.de Wenn Sie ein Software-Update durchführen, spielen Sie auf **X4000** ein neues Software-Image (Boot-Image) ein. Jedes Boot-Image beinhaltet neue Funktionen, bessere Performance und bei Bedarf Bugfixes der vorhergehenden Version. Die aktuellen von BinTec Communications AG kostenlos zur Verfügung gestellten Software-Images finden Sie über das World Wide Web unter www.bintec.de. Hier finden Sie auch aktuelle produktspezifische Dokumentation (Release Notes, Handbücher, Kurzanleitungen) und produktübergreifende Dokumentation (Software Reference, Extended Feature Reference, BRICKware for Windows).



Wenn Sie ein Software-Update durchführen, beachten Sie unbedingt die dazugehörige Release Note. Hier sind die Änderungen beschrieben, die mit dem neuen Boot-Image zur Verfügung stehen.

update Es gibt verschiedene Möglichkeiten, ein Software-Update durchzuführen. In diesem Kapitel erfolgt das Update mit Hilfe des update-Kommandos auf der SNMP-Shell und wird Schritt für Schritt genau beschrieben. Weitere Möglichkeiten finden Sie in der [Software Reference](#) und in Kap. Boot-Sequenz (siehe [Kapitel 3.5, Seite 66](#)).



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 **X4000** nicht mehr bootet!

➤ Aktualisieren Sie Modullogik, Bootmonitor oder Firmware Logic nur, wenn BinTec Communications AG eine explizite Empfehlung dazu ausspricht!

ToDo Gehen Sie folgendermaßen vor, um ein Software-Update (Boot-Image) durchzuführen:



Schalten Sie **X4000** nicht aus, während das Update durchgeführt wird!

Deaktivieren Sie vor Durchführung des Updates den Autologout mit Eingabe von `t 0` in der SNMP-Shell.

- Geben Sie die URL `www.bintec.de` in Ihren Browser (z. B. Internet Explorer oder Netscape Navigator) ein.
Die BinTec-Homepage erscheint.
- Klicken Sie auf "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 **X4000**.
- 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 Name 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 6.2, Seite 113](#)). Aktivieren Sie den TFTP-Server.
Unix-Rechner: Beachten Sie die Hinweise in der [Software Reference](#).
- Loggen Sie sich auf **X4000** 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 **X4000** 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.



X4000 benötigt einen zusammenhängenden Block an freiem Arbeitsspeicher, der etwas größer als das neue Software-Image ist. Wenn auf **X4000** nicht genügend Arbeitsspeicher zu Verfügung steht, bietet **X4000** ein incremental update an, wobei das Image "häppchenweise" direkt und ohne Überprüfung in den Flash-Speicher geladen wird. Gehen Sie folgendermaßen vor:

Wenn zu wenig Arbeitsspeicher verfügbar ist, erscheint in der SNMP-Shell:
 Do you want to perform an incremental update (y or n)?

- Geben Sie zunächst `n` ein.
 - Geben Sie `update -v <IP-Adresse> <Dateiname>` ein.
 Das Image wird überprüft, noch nicht geladen.
 - Geben Sie `update <IP-Adresse> <Dateiname>` ein.
 In der SNMP-Shell erscheint: Perform update (y or n)?
 - Geben Sie `y` ein und bestätigen Sie mit der **Eingabetaste**.
X4000 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**.
X4000 startet mit dem neuen Boot-Image. Die vorhandene Konfiguration wird überschrieben.

12 Troubleshooting

Tips Wenn Sie Probleme mit **X4000** haben, helfen Ihnen die folgenden Tips häufig schon weiter:

- Loggen Sie sich auf **X4000** 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 **X4000** erzeugten Syslog-Messages (siehe [Kapitel 10.1.1, Seite 320](#)). 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-Messages siehe [Software Reference](#).

Was die Ursachen für spezielle Probleme sein können und wie Sie dies herausfinden, zeigt Ihnen dieses Kapitel. Es ist folgendermaßen gegliedert:

- Hilfsmittel zum Troubleshooting
- Typische Fehlersituationen

12.1 Hilfsmittel zum Troubleshooting

Hier finden Sie Methoden, um die Ursache Ihres Problems einzugrenzen:

- Eingabetasten und Display zur Bedienung des Man Machine Interface (MMI)
- Lokale SNMP-Shell-Kommandos
- Externe Hilfsmittel

12.1.1 Man Machine Interface (MMI)

Mit dem MMI können Sie sich über das Display einige Informationen über den Status von **X4000** (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 Displaymeldungen intuitiv folgen. Eine detaillierte Beschreibung finden Sie in [Kapitel 5, Seite 93](#).

12.1.2 Lokale SNMP-Shell-Kommandos

Diese Kommandos geben Sie direkt in die SNMP-Shell von **X4000** ein:

debug

Mit dem Kommando `debug` können Sie die Fehlersuche für eines oder mehrere Subsysteme von **X4000** betreiben. Eine genaue Erläuterung der Syntax und der Optionen finden Sie in [Kapitel 14.1, Seite 428](#).

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 11, Seite 379](#)).



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 14.1, Seite 428](#).

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 14.1, Seite 428](#).

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 **X4000s** MAC-Adresse über das LAN zum Host mit der MAC-Adresse 0:a0:f9:d:5:a verschickt werden.

12.1.3 Externe Hilfsmittel

Mit den folgenden Hilfsprogrammen können Sie von einem Windows-PC oder einem Unix-Rechner aus Verbindungen mit **X4000** analysieren.

DIME Tracer (Windows)

Der DIME Tracer ermöglicht, **X4000s** 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 **X4000s** 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 14.2, Seite 435](#).

12.2 Typische Fehlersituationen und Vorgehensweise

Im Folgenden finden Sie eine Zusammenstellung typischer Fehlersituationen und Hinweise zu Diagnose und "Heilung". Versuchen Sie, das auftretende Problem einzugrenzen. Folgende Kategorien stehen zur Verfügung:

- System-Fehler
- ISDN-Verbindungen
- IPX-Routing

12.2.1 System-Fehler

Ich habe mein Paßwort vergessen.

Sie müssen **X4000** in den unkonfigurierten Anfangszustand (Auslieferungszustand) zurückversetzen, wie er ausgeliefert wurde:

- Verbinden Sie Ihren Rechner über die serielle Schnittstelle mit **X4000** wie in [Kapitel 3.3, Seite 59](#) beschrieben.
- Schalten Sie **X4000** aus und wieder ein.
Sie sehen diverse Selbsttests und dann "Press <sp> for boot monitor or any other key to boot system".
- Drücken Sie nun die Leertaste.
Ein BOOTmonitor-Menü wird angezeigt.
- Wählen Sie "(4) Delete Configuration" und bestätigen Sie mit der **Eingabetaste**. Beachten und bestätigen Sie die nachfolgenden Sicherheitsabfragen.
Sowohl das Paßwort als auch die komplette Konfiguration von **X4000** werden gelöscht.
- Wählen Sie "(1) Boot System".
X4000 wird neu gestartet.
- Konfigurieren Sie **X4000** erneut.

Ich kann **X4000** 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 **X4000**.
- 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 71](#)). Wenn Sie die Standard-Einstellungen im BOOTmonitor verändert haben, passen Sie Ihre Terminaleinstellungen daran an.
- Wenn Sie keinen Erfolg haben, gehen Sie vor wie unter "[Ich habe mein Paßwort vergessen.](#)", [Seite 395](#) beschrieben.

12.2.2 ISDN-Verbindungen

Hier finden Sie mögliche Fehlerquellen für ISDN-Verbindungen.

Die Telefonrechnung ist ungewöhnlich hoch.



Nutzen Sie die Funktion Taschengeldkonto (siehe [Kapitel 10.1.3, Seite 328](#)). Damit können Sie für Verbindungen mit **X4000** ein Limit festlegen, um Gebühren aufgrund von Fehlern bei der Konfiguration in Grenzen zu halten.

Möglicherweise gibt es auf **X4000** 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 **X4000** eingetragen ist.
- Überprüfen Sie mit `debug all` oder `trace`, ob ein Rechner im LAN mit einer falschen IP-Adresse für Remote-CAPI konfiguriert ist (Zielport 2662).
- Überprüfen Sie in **SYSTEM** ➤ **EXTERNAL SYSTEM LOGGING**, ob **X4000** so konfiguriert ist, daß Syslog-Messages auf einen Host außerhalb des LANs geschickt werden (Zielport 514).
- Überprüfen Sie in **IP** ➤ **STATIC SETTINGS**, ob für **X4000** unter **Time Server** eine IP-Adresse eingetragen wurde, die außerhalb des LANs liegt.
- Überprüfen Sie in der MIB-Tabelle **biboAdmTrapHostTable**, ob **X4000** so konfiguriert ist, daß SNMP-Traps auf einen Host außerhalb des LANs geschickt werden (Zielports 161, 162).
- Überprüfen Sie, ob bei Verbindungen mit dynamischem Channel Bundling häufiges Auf- und Abbauen des zweiten B-Kanals aufgrund von schwankendem Traffic geschieht.
- Überprüfen Sie mit `debug all` oder `trace`, ob ein Rechner im LAN mit einer falschen IP-Adresse für den WINS-Server konfiguriert ist (Zielports 137-139). Konfigurieren Sie gegebenenfalls den Rechner richtig oder setzen Sie entsprechende Filter ein.
- Überprüfen Sie mit `debug all` oder `trace`, ob ein Rechner im LAN für Namensauflösung von NetBIOS-Namen mit Hilfe von DNS konfiguriert ist (es wird von einem Clientport aus auf Zielport 53 zugegriffen). Versuchen Sie nicht, NetBIOS-Namen mit DNS aufzulösen!
- Überprüfen Sie mit `debug all` oder `trace`, ob eine Applikation auf einem Rechner im LAN versucht, Adressen aufzulösen, die der Name-Server beim Internet Service Provider nicht kennt (es wird von einem Clientport aus auf Zielport 53 zugegriffen). Richten Sie eine lokale HOSTS-Datei im Windows-Verzeichnis ein, die die Namensauflösung durchführen kann.
- Überprüfen Sie mit `debug all` oder `trace`, ob auf einem Rechner im LAN NetBIOS over IP eingerichtet ist (es wird vom Sourceport 137 auf den Zielport 53 zugegriffen). Dabei wird versucht, NetBios-Namen über DNS auf-

zulösen. Schalten Sie NetBIOS over IP ab oder setzen Sie Filter ein (Konfiguration der entsprechenden Filter finden Sie in [Kapitel 10.2.8, Seite 349](#) oder nutzen Sie den einfachen NetBIOS-Filter des Configuration Wizards, siehe [Kapitel 6, Seite 109](#)).

- Überprüfen Sie, ob Sie Callback konfiguriert haben (siehe [Kapitel 10.2.4, Seite 341](#)) 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.

12.2.3 IPX-Routing

Hier finden Sie einige Probleme mit dazugehörigen Lösungsvorschlägen, die bei IPX-Routing auftreten könnten.

- Überprüfen Sie mit dem Setup Tool oder dem MMI, ob Sie die richtige Lizenz eingetragen haben.
- Überprüfen Sie mit dem Setup Tool, ob in **IPX** der Eintrag unter **Internal Network Number** im LAN eindeutig ist.

Ein Server existiert in einem Remote-LAN (LAN-LAN-Kopplung über ISDN), aber ist für Clients im lokalen LAN "unsichtbar".

Der Server könnte für Clients unsichtbar sein, weil SAP-Pakete vom Server nicht empfangen werden:

- Überprüfen Sie die Eintragungen von **Update Time** und **Age Multiplier** in **WAN PARTNER** ➤ **EDIT** ➤ **IPX**. Die Einstellungen müssen zu den Einstellungen auf den Servern im **X4000**-LAN kompatibel sein.
- Überprüfen Sie, ob ein dazwischenliegender Router die SAP-Pakete ausfiltert.
- Überprüfen Sie mit isdnlogin, ob eine ISDN-Verbindung zwischen Client und Server zustande kommen kann.
- Überprüfen Sie, ob Sie unter **CM-100BT**, **FAST ETHERNET** die **local IPX-NetNumber** und **Encapsulation** richtig eingetragen haben und ob der Server sie empfangen kann.

Wenn der Client versucht, einen Server in einem Remote-Netzwerk über eine PPP-Verbindung zu erreichen, wartet er sehr lange und die Verbindung wird evtl. abgebrochen.

In manchen Fällen meldet der lokale Router dem Client fälschlicherweise, daß ein Server erreichbar ist.

- Überprüfen Sie, ob der Server abgestürzt und das Aging-Intervall noch nicht abgelaufen ist. Verändern Sie gegebenenfalls die Einstellung von **Send RIP/SAP Updates** unter **WAN PARTNER** ➤ **EDIT** ➤ **IPX**.
- Überprüfen Sie, ob der Server und der Router im Remote-Netzwerk gleichzeitig inaktiv sind (z. B. wegen Stromausfall). Setzen Sie die WAN-Schnittstelle des entsprechenden WAN-Partners mit dem Befehl `ifconfig` kurz auf `down` und anschließend wieder auf `dialup`, um die vom WAN-Partner gelernten Routen und Dienste zu löschen.

Ich kann auf dem Client nicht auf ein Netz-Laufwerk des Clients wechseln.

- Möglicherweise ist der Server für den Client unsichtbar. Gehen Sie vor wie unter "Ein Server existiert in einem Remote-LAN ..." beschrieben.
- Überprüfen Sie, ob die auf dem Server zur Verfügung stehenden Lizenzen alle belegt sind.

ISDN-Verbindungen werden ständig neu aufgebaut.

Es sind nicht nur RIP/SAP-Pakete, die den Aufbau von ISDN-Verbindungen verursachen.

- Überprüfen Sie, ob sich ein Eintrag in der MIB-Tabelle **ipxDenyTable** befindet, der verhindert, daß Novell Serialization-Pakete über die Wahlverbindung gesendet werden.
- Überprüfen Sie, ob Sie unter **IPX enable IPX spoofing** und **enable SPX spoofing** mit `yes` aktiviert haben.
- Überprüfen Sie, ob irgendwo RCONSOLE mit einem ständig sich verändernden Bildschirm (z. B. MONITOR, IPXCON, TCPCON, ein Bildschirm-schoner, usw.) aktiv ist.

- Überprüfen Sie, ob im LAN NetBIOS over IPX verwendet wird (Windows for Workgroups, NT, Win95). Wählen Sie gegebenenfalls unter **IPX** für **NetBIOS Broadcast replication** *no* oder *on LAN only* aus.
- Überprüfen Sie, ob NDS Replica Synchronisation aktiv ist (ab Netware 4.1 Server).
- Werten Sie die Syslog-Messages (**Level** = *debug*) aus und filtern Sie gegebenenfalls die IPX-Pakete aus, die dort als Ursache für ungewollte Verbindungsaufbauten genannt werden.

Die MIB-Variable **ipxAdmSpxConns** enthält mehr Verbindungen als tatsächlich aktiv sind.

X4000 empfängt möglicherweise keine SPX-Abbruch-Meldungen vom Server:

- Geben Sie das Kommando `reset router` an der Konsole des entsprechenden Servers ein.
Alle inaktiven Verbindungen zwischen dem Server und **X4000** werden abgebaut.
- Bei fehlender Abmeldung könnten SPX-Verbindungen noch bis zu einem Timeout bestehen und dadurch in **ipxAdmSpxConns** mitgezählt werden.

13 Technische Daten

Allgemeine Produktmerkmale:

Bezeichnung	Wert
Abmessungen: Desktop-Gerät 19-Zoll-Einbaugerät	B x H x T in mm 105 x 260 x 300 220 x 44 x 290
Gewicht: Desktop-Gerät 19-Zoll-Einbaugerät	2,6 kg 2,1 kg
Transportgewicht (inkl. Dokumentation, Kabel, Verpackung): Desktop-Gerät 19-Zoll-Einbaugerät	5,1 kg 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 13-1: Technische Daten von **X4000**

13.1 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 13-2: Technische Daten des Netzteils

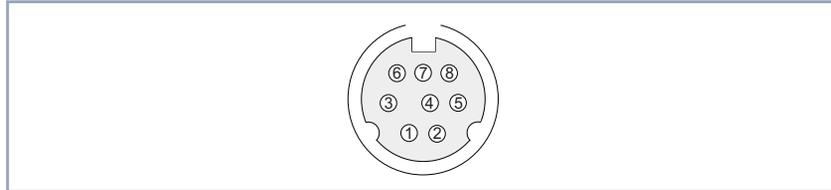
13.2 Leistungsmerkmale des Grundgeräts

Bezeichnung	Wert
Prozessor	Motorola MPC860T RISC CPU
Speicher	16 MB SDRAM 4 MB Flash-ROM
Schnittstellen: Konsolenschnittstelle Ethernet/LAN-Schnittstelle WAN-Schnittstellen	Seriell, Mini-DIN 10/100 Base-T Auto-Sensing, RJ45-Buchse ISDN-Schnittstelle BRI S/T, RJ45-Buchse 2 x X.21/V.35/V.36/X.21bis, 26-polige Mini Delta Ribbon Buchse, bis 2048 kBit/s
Anzeigen	grün beleuchtetes 122 x 132-Pixel-LCD-Display mit beleuchteten Einbabetasten blaue Power-LED auf der Frontblende von X4000 2 Status-LEDs, grün und rot, auf der Rückseite von X4000
Erweiterbarkeit	Steckplatz für eine X4000 -Erweiterungskarte

Tabelle 13-3: Leistungsmerkmale des Grundgeräts

13.2.1 Serielle Konsolenschnittstelle

Die Pin-Belegung der seriellen Konsolenschnittstelle des Grundgeräts (8-polige MiniDin-Buchse):

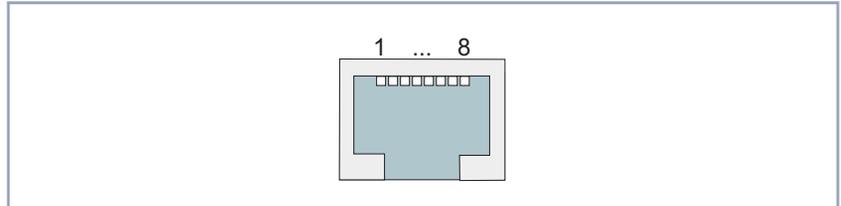


1	Für Testzwecke	5	RXD
2	Für Testzwecke	6	NC
3	TXD	7	NC
4	GND	8	NC

Bild 13-1: Serielle Konsolenschnittstelle mit Pin-Belegung

13.2.2 Ethernet/LAN-Schnittstelle

Die Pin-Belegung der 10/100 Base-T Ethernet/LAN-Schnittstelle des Grundgeräts (RJ45-Buchse):



1	T+	5	Schirm
2	T-	6	R-
3	R+	7	Schirm
4	Schirm	8	Schirm

Bild 13-2: 10/100 Base-T Ethernet/LAN-Schnittstelle (RJ45-Buchse) des Grundgeräts mit Pin-Belegung

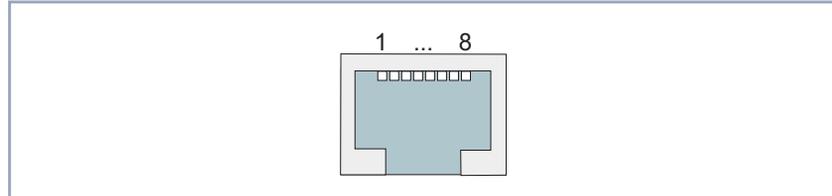
Das zu verwendende LAN-Kabel muß die folgenden technischen Merkmale erfüllen:

- 100 Base-T-Kabel CAT5 STP (Shielded Twisted Pair)
- Beidseitig vollständig abgeschirmter 8-poliger RJ45-Stecker
- 4 verdrehte Aderpaare zu je 2 Adern; folgende Adern sind verdreht:
 - Pin 1+2
 - Pin 3+6
 - Pin 4+5
 - Pin 7+8

Gesamtschirmung um alle vier Aderpaare.

13.2.3 ISDN-BRI-Schnittstelle

Die Pin-Belegung der ISDN-BRI-Schnittstelle (RJ45-Buchse):



1	NC	5	R-
2	NC	6	T-
3	T+	7	NC
4	R+	8	NC

Bild 13-3: ISDN-BRI-Schnittstelle (RJ45-Buchse) des Grundgeräts mit Pin-Belegung

13.2.4 Serielle WAN-Schnittstellen

Das **X4000**-Grundgerät verfügt über zwei serielle WAN-Schnittstellen:

- Der erste serielle Port (Setup-Tool-Menü **CM-SERIAL**, **SERIAL** ► **UNIT 0**) ist als Schnittstelle der Typen
 - X.21/V.11
 - V.35/V.11
 - V.36/V.11verwendbar.
Durch die Einstellung im Setup-Tool-Feld **Connector** (siehe [Tabelle 7-11](#), [Seite 155](#)) kann der Port so umgestellt werden, daß **X4000** 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.

- Der zweite serielle Port (Setup-Tool-Menü **CM-SERIAL**, **SERIAL** ► **UNIT 1**) ist als Schnittstelle des Typs
 - X.21bis/V.28verwendbar.
Bei diesem Port kann die Umstellung vom DCE- in den DTE-Modus und umgekehrt nur über die Verwendung eines DCE- bzw. DTE-Kabels verwirklicht werden.

Die zu verwendenden Kabel sind nicht im Lieferumfang von **X4000** 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!

Im folgenden werden zunächst die Stecker beschrieben, die für X.21, V.35, V.36 bzw. X.21bis in der Regel verwendet werden:

- "DB-15-Stecker für X.21", [Seite 411](#))

- "M34-Stecker für V.35", Seite 412)
- "DB-37-Stecker für V.36", Seite 413
- "DB-25-Stecker für X.21bis", Seite 415)

Anschließend werden die beiden seriellen **X4000**-Ports beschrieben, über die die genannten Schnittstellen bei **X4000** realisiert werden:

- "26-polige Mini-Delta-Ribbon-Buchse für X.21, V.35 und V.36", Seite 416)
- "20-polige Mini-Delta-Ribbon-Buchse für X.21bis", Seite 419

DB-15-Stecker für X.21

Für eine X.21-Schnittstelle wird in der Regel ein DB-15-Stecker nach ISO 4903 verwendet:

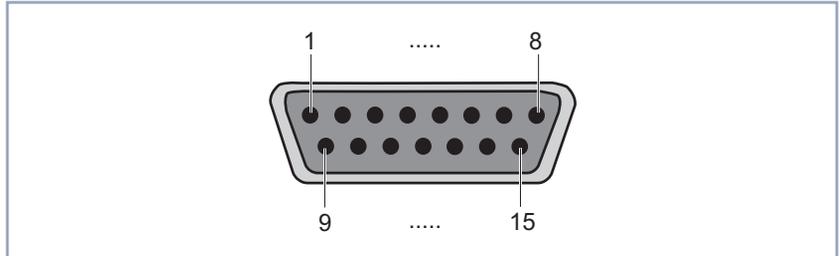


Bild 13-4: DB-15-Stecker (DTE)

Die Pins des DB-15-Steckers (DTE) bzw. -Buchse (DCE) sind folgendermaßen belegt:

Variable Connector=DTE		Signalrichtung Pin-Nr.	Variable Connector=DCE	
ITU-T	Signal		Signal	ITU-T
101	PG	— 1 —	PG	101
102	SG	— 8 —	SG	102
103	T+	9 —>	R+	104
103	T-	2 —>	R-	104
104	R+	<— 11	T+	103
104	R-	<— 4	T-	103
105	C+	10 —>	I+	106
105	C-	3 —>	I-	106
106	I+	<— 12	C+	105
106	I-	<— 5	C-	105
115	S+	<— 13	S+	114
115	S-	<— 6	S-	114

Tabelle 13-4: Pin-Belegung eines DB-15-Steckers für X.21 (ISO 4903)

M34-Stecker für V.35

Für eine V.35-Schnittstelle wird in der Regel ein M34-Stecker nach ISO 2593 verwendet:

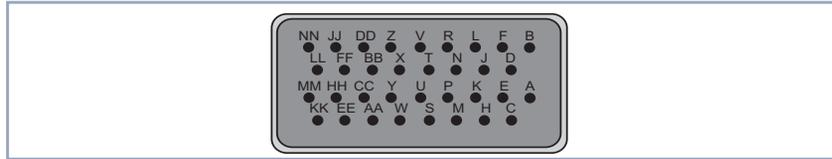


Bild 13-5: M34-Stecker

Die Pins des M34-Steckers sind folgendermaßen belegt:

Variable Connector=DTE		Signalrichtung Pin-Nr.	Variable Connector=DCE	
ITU-T	Signal		Signal	ITU-T
101	ChGND	— A —	ChGND	101
102	SigGND	— B —	SigGND	102
103	TDA	P —>	RDA	104
103	TDB	S —>	RDB	104
104	RDB	<— R	TDB	103
104	RDA	<— T	TDA	103
105	RTS	C —>	CTS	106
106	CTS	<— D	RTS	105
115	RCA	<— V	TCA	114
115	RCB	<— X	TCB	114
108/2	DTR	H —>	DSR	107
109	DCD	<— F	DCD	109
107	DSR	<— E	DTR	108/2
114	TCB	<— Y	TCB	114
114	TCA	<— AA	TCA	114

Tabelle 13-5: Pin-Belegung eines M34-Steckers für V.35 (ISO 2593)

DB-37-Stecker für V.36

Für eine V.36-Schnittstelle wird in der Regel ein DB-37-Stecker nach ISO 4902 verwendet:

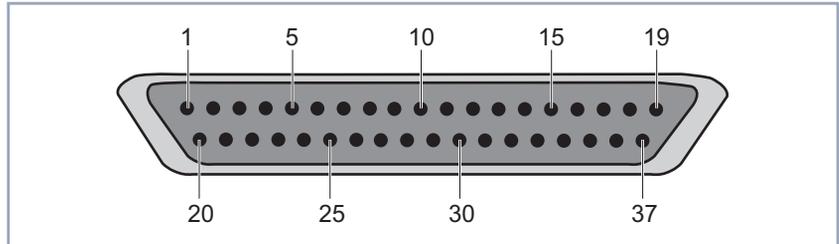


Bild 13-6: DB-37-Stecker

Die Pins des DB-37-Steckers sind folgendermaßen belegt:

Variable Connector=DTE		Signalrichtung Pin-Nr.	Variable Connector=DCE	
ITU-T	Signal		Signal	ITU-T
101	ChGND	— 1 —	ChGND	101
102	SigGND	— 19 —	SigGND	102
103	TDB	22 —>	RDB	104
103	TDA	4 —>	RDA	104
104	RDB	<— 24	TDB	103
104	RDA	<— 6	TDA	103
105	RTSB	25 —>	RTSB	106
105	RTSA	7 —>	CTSA	106
106	CTSB	<— 27	RTSB	105
106	CTSA	<— 9	RTSA	105
115	RCB	<— 26	TCB	114
115	RCA	<— 8	TCA	114
108/2	DTRB	30 —>	DSRB	107
108/2	DTRA	12 —>	DSRA	107
109	DCDB	<— 31	DCDB	109
109	DCDA	<— 13	DCDA	109
107	DSRB	<— 29	DTRB	108/2
107	DSRA	<— 11	DTRA	108/2
114	TCB	<— 23	TCB	114
114	TCA	<— 5	TCA	114

Tabelle 13-6: Pin-Belegung eines DB-37-Steckers für V.36 (ISO 4902)

DB-25-Stecker für X.21bis

Für eine X.21bis-Schnittstelle wird in der Regel ein DB-25-Stecker nach ISO 2110 verwendet:

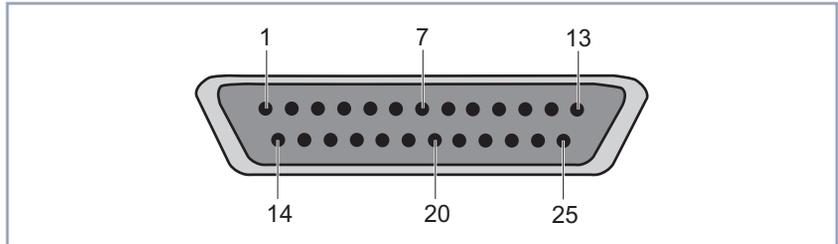


Bild 13-7: DB-25-Stecker

Die Pins des DB-25-Steckers sind folgendermaßen belegt:

DTE-Kabel		Signalrichtung Pin-Nr.	DCE-Kabel	
ITU-T	Signal		Signal	ITU-T
101	ChGND	—— 1 ——	ChGND	101
103	TD	2 ——>	RD	104
104	RD	<—— 3	TD	103
105	RTS	4 ——>	CTS	106
106	CTS	<—— 5	RTS	105
107	DSR	<—— 6	DTR	108/2
102	SigGND	—— 7 ——	SigGND	102
109	DCD	<—— 8	DCD	109
114	TxC	<—— 15	TxC	114
115	RxC	<—— 17	RxC	115
108/2	DTR	20 ——>	DSR	107
113	XTC	24 ——>	RxC / TxC	114/115
	VCC +5V	—— 25 ——	VCC +5V	

Tabelle 13-7: Pin-Belegung eines DB-25-Steckers für X.21bis (ISO 2110)

26-polige Mini-Delta-Ribbon-Buchse für X.21, V.35 und V.36

Die serielle X.21/V.35/V.36-Schnittstelle von **X4000** ist als 26-polige Mini-Delta-Ribbon-Buchse ausgeführt. Je nach Einstellung unter **Interface Type** kann die Schnittstelle für X.21, V.35 oder V.36 verwendet werden.

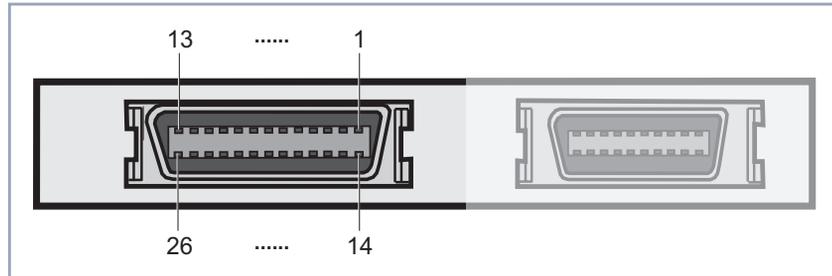


Bild 13-8: 26-polige Mini-Delta-Ribbon-Buchse (erster serieller Port, links)

Die Pins der 26-poligen Mini-Delta-Ribbon-Buchse sind im DTE-Modus (**Connector = DTE**) folgendermaßen belegt:

ITU-T	Richtung und Pin-Nr.	X.21-Pin (DB-15)		V.35-Pin (M34)		V.36-Pin (DB-37)	
101	— 1 —	1	PG	A	ChGND	1	ChGND
102	— 2 —	8	SG	B	SigGND	19	SigGND
103	3 —>	9	T+	S	TDB	22	TDB
103	4 —>	2	T-	P	TDA	4	TDA
104	<— 5	11	R+	T	RDB	24	RDB
104	<— 6	4	R-	R	RDA	6	RDA
105	7 —>	10	C+			25	RTSB
105	8 —>	3	C-	C	RTS	7	RTSA
106	<— 9	12	I+			27	CTSB
106	<— 10	5	I-	D	CTS	9	CTSA
115	<— 11	13	S+	X	RCB	26	RCB
115	<— 12	6	S-	V	RCA	8	RCA
108/2	15 —>					30	DTRB
108/2	16 —>			H	DTR	12	DTRA
109	<— 17					31	DCDB
109	<— 18			F	DCD	13	DCDA
107	<— 19					29	DSRB
107	<— 20			E	DSR	11	DSRA
114	<— 21			AA	TCB	23	TCB
114	<— 22			Y	TCA	5	TCA
VCC+5V	— 25 —						

Tabelle 13-8: Pin-Belegung der 26-poligen Mini-Delta-Ribbon-Buchse (DTE-Modus)

Die Pins der 26-poligen Mini-Delta-Ribbon-Buchse sind im DCE-Modus (**Connector = DCE**) folgendermaßen belegt:

ITU-T	Richtung und Pin-Nr.	X.21-Pin (DB-15)		V.35-Pin (M34)		V.36-Pin (DB-37)	
101	— 1 —	1	PG	A	ChGND	1	ChGND
102	— 2 —	8	SG	B	SigGND	19	SigGND
104	3 —>	9	R+	S	RDB	22	RDB
104	4 —>	2	R-	P	RDA	4	RDA
103	<— 5	11	T+	T	TDB	24	TDB
103	<— 6	4	T-	R	TDA	6	TDA
106	7 —>	10	I+			25	RTSB
106	8 —>	3	I-	C	CTS	7	CTSA
105	<— 9	12	C+			27	RTSB
105	<— 10	5	C-	D	RTS	9	RTSA
114	<— 11	13	S+	X	TCB	26	TCB
114	<— 12	6	S-	V	TCA	8	TCA
107	15 —>					30	DSRB
107	16 —>			H	DSR	12	DSRA
109	<— 17					31	DCDB
109	<— 18			F	DCD	13	DCDA
108/2	<— 19					29	DTRB
108/2	<— 20			E	DTR	11	DTRA
114	<— 21			AA	TCB	23	TCB
114	<— 22			Y	TCA	5	TCA
VCC+5V	— 25 —						

Tabelle 13-9: Pin-Belegung der 26-poligen Mini-Delta-Ribbon-Buchse (DCE-Modus)

20-polige Mini-Delta-Ribbon-Buchse für X.21bis

Die serielle X.21bis-Schnittstelle von **X4000** ist als 20-polige Mini-Delta-Ribbon-Buchse ausgeführt.

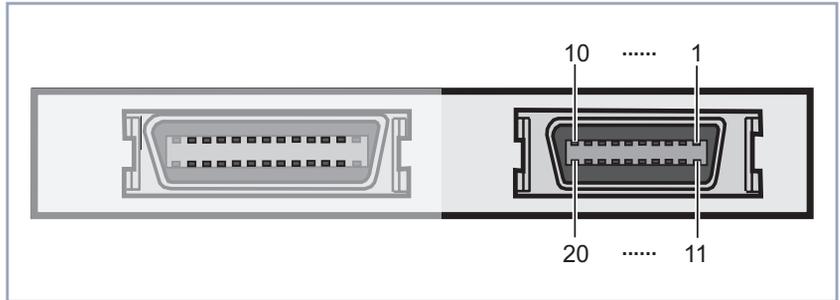


Bild 13-9: 20-polige Mini-Delta-Ribbon-Buchse (zweiter serieller Port, rechts)

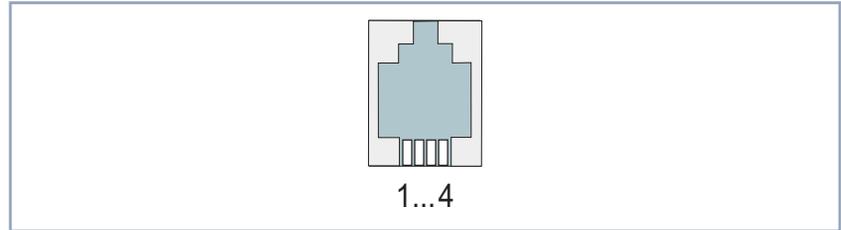
Die Pins der 20-poligen Mini-Delta-Ribbon-Buchse sind folgendermaßen belegt (für DTE-Modus ist ein DTE-Kabel erforderlich, für DCE-Modus ein DCE-Kabel):

DTE/DCE			
ITU-T	Signal	Signalrichtung Pin-Nr.	X.21bis (DB-25)
101	ChGND	— 1 —	1
103	TD	2 —>	2
104	RD	<— 3	3
105	RTS	4 —>	4
106	CTS	<— 5	5
107	DSR	<— 6	6
102	SigGND	— 7 —	7
109	DCD	<— 8	8
108/2	DTR	9 —>	20
113	XTC	11 —>	24
114	TxC	<— 12	15
115	RxC	<— 13	17
	VCC +5V	— 14 —	

Tabelle 13-10: Pin-Belegung der 26-poligen Mini-Delta-Ribbon-Buchse

13.2.5 Display-Schnittstelle

Die RJ11-Buchse für den Display-Stecker ist mit folgender Pin-Belegung ausgeführt:



1	VDD: +3.3V Versorgungsspannung	3	SDA: I ² C Serial Data
2	SCL: I ² C Serial Clock	4	GND

Bild 13-10: RJ11-Buchse für Display-Stecker mit Pin-Belegung

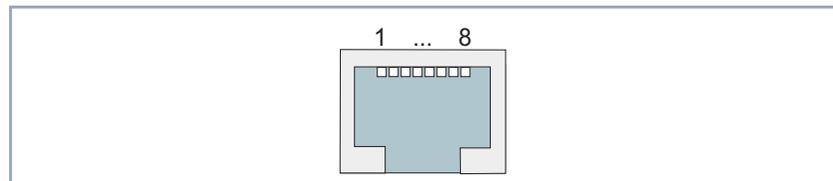
13.3 Leistungsmerkmale der Erweiterungs- und Ressourcenkarten

13.3.1 X4E-2/3BRI – WAN-Schnittstellenkarte für ISDN-BRI (Basic Rate Interface)

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 13-11: Leistungsmerkmale der BRI-Erweiterungskarte

Pinbelegung 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

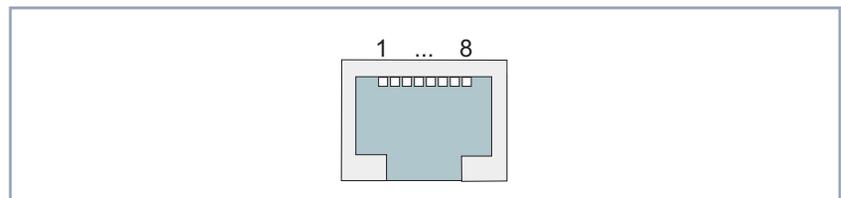
Bild 13-11: ISDN-BRI-Schnittstelle (RJ45-Buchse) der BRI-Erweiterungskarte

13.3.2 X4E-1/2PRI – WAN-Schnittstellenkarte für ISDN-PRI (Primary Rate Interface) und/oder G.703

Bezeichnung	Wert
Schnittstellen	2 x Schnittstelle für ISDN-PRI/G.703 mit jeweils 2 Buchsen (IN und OUT) Beim Abschalten von X4000 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 13-12: Leistungsmerkmale der PRI-/G.703-Erweiterungskarte

Pinbelegung Die Pins der ISDN-PRI-/G.703-Schnittstellen sind folgendermaßen belegt:



1	R+	5	T-
2	R-	6	NC
3	NC	7	NC
4	T+	8	NC

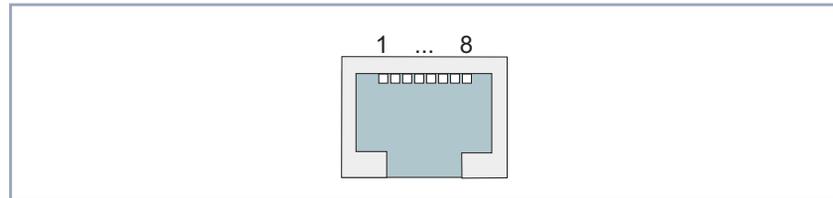
Bild 13-12: ISDN-PRI-/G.703-Schnittstelle (RJ45-Buchse) der PRI-/G.703-Erweiterungskarte

13.3.3 X4E-2FE – LAN-Schnittstellenkarte für 10/100 MBit/s

Bezeichnung	Wert
Schnittstellen	2 x 10/100 Base-T Auto-Sensing
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 13-13: Leistungsmerkmale der LAN-Erweiterungskarte

Pinbelegung 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 13-13: LAN-Schnittstelle (RJ45-Buchse) der LAN-Erweiterungskarte

13.3.4 XTR-S/M/L – Ressourcenkarten mit Digitalmodems

Die Ressourcenkarten mit Digitalmodems sind in folgenden Ausführungen für X4E-3BRI und X4E-2PRI erhältlich:

- XTR-S mit 8 Digitalmodems
- XTR-M mit 12 Digitalmodems
- XTR-L mit 30 Digitalmodems

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 13-14: Leistungsmerkmale der Ressourcenkarten mit Digitalmodems



Bei Verwendung einer Erweiterungskarte mit Ressourcenkarte(n) im **X4000**-Einbaugerät empfiehlt BinTec Communications AG die Verwendung der optional erhältlichen Lüfterkassette.

13.3.5 XTR-ENC – Ressourcenkarte zur Verschlüsselung und Kompression

Die Ressourcenkarten zur Verschlüsselung und Kompression bietet eine Hardwareunterstützung für STAC-Kompression und symmetrische Verschlüsselung. Unterstützte Verschlüsselungsverfahren: DES, 3DES, CAST, Twofish und Blowfish.

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 13-15: Leistungsmerkmale der Ressourcenkarte zur Verschlüsselung und Kompression

Die ISDN-PRI- bzw. G.703-Erweiterungskarte ist im Auslieferungszustand standardmäßig mit Hardwareunterstützung für Verschlüsselung und Kompression ausgestattet, die ISDN-BRI-Erweiterungskarte sowie die LAN-Erweiterungskarte kann 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.



Bei Verwendung einer Erweiterungskarte mit Ressourcenkarte(n) im **X4000**-Einbaugerät empfiehlt BinTec Communications AG die Verwendung der optional erhältlichen Lüfterkassette.

14 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

14.1 SNMP-Shell-Kommandos

Auf **X4000** 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 über die wichtigsten Kommandos, verfügbar auf **X4000**, angezeigt.



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 oder X.21-Schnittstelle, 1 ... 31 = Bx-Kanal.
- `unit`: 0 ... 1. Selektieren des physikalischen Interface für Module mit zwei Interfaces (z. B. CM-2BRI).
- `slot`: 1 ... 2. Angabe des Slot, in dem das Modul installiert ist.
- `next`: Nur Informationen über den als nächstes geöffneten B-Kanal anzeigen.
- `<ifcname>`: Name oder Index der Schnittstelle (siehe "ifstat", Seite 432).
- `-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` = **X4000**'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 **X4000** 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 **X4000s** 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 <destaddr>] [<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 <destaddr>`: Ziel-IP-Adresse eines Hosts. Damit wird eine Host-Route zu diesem Host in die Routing-Tabelle hinzugefügt (**ipRouteDest**).
- `address: X4000s` IP-Adresse für die Schnittstelle (**ipRouteNextHop**).
- `netmask <mask>`: Netzmaske der Schnittstelle (**ipRouteMask**).
- `up`: Setzt die Schnittstelle auf den Status up.
- `down`: Setzt die Schnittstelle auf den Status down.
- `dialup`: Setzt die Schnittstelle auf den Status dialup.
- `-`: Definiert keine eigene IP-Adresse (**ipRouteNextHop = 0.0.0.0**).
- `metric <n>`: Setzt Metrik der Route auf n (**ipRouteMetric1**).

ifstat

```
ifstat [-lur] [<ifcname>]
```

Wird benutzt, um Statusinformationen über die Schnittstellen des Systems anzuzeigen (basierend auf den Eintragungen in der MIB-Tabelle **ifTable**).

- `-l`: Zeigt Informationen der Schnittstelle in voller Länge an (normalerweise wird die Beschreibung nur bis zum 12. Zeichen angezeigt).
- `-u`: Zeigt nur Informationen über die Schnittstellen an, die den Status up haben.
- `-r`: Zeigt die Filter an, die für die Schnittstelle definiert sind.
- `ifcname`: Zeigt nur Informationen zu den Schnittstellen an, deren Namen mit den eingegebenen Zeichen beginnen (z. B. `ifstat en1` zeigt Informationen zu den Schnittstellen `en1`, `en1-llc` 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]`

X4000 hat eine Software-Uhr. Mit Eingabe von `date` wird die eingestellte Uhrzeit angezeigt.

Mit Eingabe von `date YYMMDDHHMMSS` stellen Sie die Uhr auf den entsprechenden Wert ein (Jahr, Monat, Tag, Stunde, Minute, Sekunde).

t

`t [<seconds>]`

Wird benutzt, um den Zeitraum für Autologout für die aktuelle Login-Session zu definieren (standardmäßig wird eine Verbindung zu **X4000** über telnet, isdnlogin oder seriell automatisch getrennt, wenn 15 Minuten lang keine Eingabe über die Tastatur erfolgt).

- `seconds`: Nach `seconds` Sekunden erfolgt der Autologout. Mit Eingabe von `t 0` deaktivieren Sie Autologout.

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 **X4000** oder einen anderen Nameserver aufgelöst wird.

- `-a`: Zeigt alle erhaltenen Daten an.

- `-n`: Verhindert die Auflösung der angegebenen Nameserver-Adresse (ohne diese Option wird versucht, die Adresse des Nameservers 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 Dezimal-Zahl.
- `-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 Nameservers, der befragt werden soll (Standardwert: 127.0.0.1). Es wird versucht, diese Nameserver-Adresse vom lokalen DNS-Proxy auflösen zu lassen.



Durch Eingabe von `-?` erhalten Sie meistens Hilfen zur Syntax.

Das Kommando `update` finden Sie in [Kapitel 11.2, Seite 388](#).

Weitere SNMP-Kommandos finden Sie in der [Software Reference](#).

14.2 BRICKtools for Unix-Kommandos

Die Programme bricktrace und capitrace sind in BRICKtools for UNIX auf der BinTec-Companion CD enthalten. Sie werden durch Eingabe der folgenden Kommandos auf einem Unix-Rechner gestartet.

bricktrace

```
bricktrace [-h23aeFpiNtxs] [-T <tei>] [-c <cref>]
[-r <cnt>] [-H <host>] [-P <port>] <channel> <unit> <slot>
```

Wird benutzt, um ISDN-Meldungen (D- und B-Kanäle) zu verfolgen und auszuwerten.

- -h: hexadezimale Ausgabe.
- -2: Schicht-2-Ausgabe.
- -3: Schicht-3-Ausgabe.
- -a: Asynchronous HDLC (nur B-Kanal).
- -e: ETS300075 (EuroFileTransfer)-Ausgabe.
- -F: Fax (nur B-Kanal).
- -p: PPP (nur B-Kanal).
- -i: IP-Ausgabe (nur B-Kanal).
- -N: Novell IPX-Ausgabe (nur B-Kanal).
- -t: Ausgabe in ASCII-Text (nur B-Kanal).
- -x: Raw dump mode.
- -s: **X4000** auf verfügbare Trace-Kanäle überprüfen.
- -T <tei>: TEI-Filter setzen (nur D-Kanal).
- -c <cref>: Callref-Filter setzen (nur D-Kanal).
- -r <cnt>: Nur cnt bytes empfangen.
- -H <host>: IP-Adresse oder Name des IP-Hosts.
- -p <port>: Spezifiziert Trace-TCP-Port (Standard: 7000).
- channel: 0 = D-Kanal oder X.21-Schnittstelle, 1 ... 31 Bx-Kanal.
- unit: 0 ... 1. Selektieren des physikalischen Interface für Module mit zwei Interfaces (z. B. CM-2BRI).
- slot: 1 ... 2. Angabe des Slot, in dem das Modul installiert ist.

capitrace

```
capitrace [-h] [-s] [-l]
```

Wird benutzt, um CAPI-Meldungen zu verfolgen und auszuwerten. Alle von **X4000** gesendeten oder empfangenen CAPI-Meldungen werden angezeigt. Als Umgebungsvariable CAPI_HOST muß die IP-Adresse von **X4000** 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>)

- 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: Internet-Zugang, 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 **X4000** 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 (Kommunikationsprogramme wie RVS-COM Lite) arbeiten mit der CAPI-Schnittstelle. Über solche Kommunikationsprogramme können Sie z. B. von Ihrem Rechner aus über das ISDN Fax 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. **X4000** 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** Einkapsulierung 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 **X4000** 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).
- 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 sog. **➤➤ S₀-Bus** geschaffen.

ISDN-BRI ISDN Basic Rate Interface

➤➤ ISDN-Basisanschluß, auch **➤➤ S₀-Anschluß**.

ISDN-Login Funktion von **X4000**. Über ISDN-Login ist **X4000** 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 **X4000**. 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 (**➤➤ MSNs**) angesprochen.

MIB Management Information Base

MIB ist eine Datenbank, die alle im Netz angeschlossenen managbaren Geräte und Funktionen beschreibt. Jede MIB (so auch die BinTec MIB) enthält herstellerspezifische Objekte. **➤➤ SNMP** setzt auf MIB auf.

MMI Man Machine Interface

Ist eine komfortable Benutzerführung mit LCD-Display und Eingabetasten, die den Anwender durch grundlegende Funktionen von **X4000** 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 **►► S₀-Bus** erlaubt. Eine MSN hat bis zu acht Stellen, z. B. 49 911 7654321, wobei die 7654321 der MSN entspricht.

In der Regel erhält man in Deutschland mit dem ISDN-Basisanschluß (Mehrgereäteanschluß) drei solcher MSNs.

Multiprotokoll-Router **►► Router**, der mehrere Protokolle routen kann, z. B. **►► IP**, **►► IPX** etc.

NAT Network Address Translation
Sicherheitsmechanismus von **X4000**. 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 (**►► S₀-Bus**) an das öffentliche ISDN-Netz. Er entspricht dem Verteilerkästchen (TAE-Dose) beim analogen Telefon-Anschluß.

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 (**S₀-Bus**) an das öffentliche ISDN-Netz. Er entspricht dem Verteilerkästchen (TAE-Dose) beim analogen Telefon-Anschluß.

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 **S₀-Schnittstelle** und **1TR6** bzw. anderen herstellerspezifischen **D-Kanal-Protokollen** auf der Teilnehmerseite.

Nebenstellenanlagen ermöglichen interne Verbindungen zwischen den Anschlüssen der TK-Anlage, ohne daß dabei auf Telefonanbieter zugegriffen werden muß. Nicht alle BinTec-Router enthalten eine Nebenstellenanlage.

PAP Password Authentication Protocol

Authentisierungsverfahren für Verbindungen über **PPP**. Funktioniert wie **CHAP**, außer daß Benutzername und Paßwort nicht verschlüsselt werden, bevor sie zum Partner übertragen werden.

Ping Packet Internet Groper

Befehl, über den man die Entfernung entfernter Netzwerkkomponenten ermitteln kann. Ping wird auch für Testzwecke verwendet, um festzustellen, ob das entfernte Gerät überhaupt erreicht werden kann.

Port Ein-/Ausgang

Anhand der Port-Nummer wird entschieden, an welche Dienste (Telnet, WWW) ein ankommendes Datepaket weitergeleitet wird.

- 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: Internet-Zugang, 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 **X4000**) 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 **X4000** auf einen einzigen ISDN-Anschluß zuzugreifen. Voraussetzung ist, daß alle Teilnehmer eine geeignete Anwendungssoftware installiert haben, die die CAPI-Schnittstelle unterstützt. Diese genormte Schnittstelle wird von den meisten Kommunikationsanwendungen verwendet.

Im Lieferumfang von **X4000** ist eine entsprechende Software (RVS-COM Lite) enthalten.

Die CAPI-Schnittstelle von BinTec ist als Dualmode-CAPI realisiert. Es können parallel CAPI 1.1- und 2.0-Anwendungen auf die ISDN-Ressourcen zugreifen. Somit können neben alten auf CAPI 1.1 basierenden Anwendungen, parallel im Netz oder auf dem gleichen Rechner, neue CAPI 2.0-Anwendungen betrieben werden.

RIP Routing Information Protocol

Routing-Protokoll, das in Netzwerken verwendet wird, um Informationen (Routing-Tabellen) zwischen >>> **Routern** auszutauschen.

RJ45 Stecker bzw. Buchse für maximal acht Adern. Anschluß für digitale Endgeräte.

Router Geräte, die unterschiedliche Netze auf der 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 **X4000** sind **Multiprotokoll-Router** und dadurch in der Lage, mehrerer 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.

S₀-Anschluß Siehe **ISDN-Basisanschluß**.

S₀-Bus Sämtliche ISDN-Anschlußdosen und der **NTBA** beim ISDN-Mehrgerätee-Anschluß. Jeder S₀-Bus besteht aus einem vieradrigen Kabel. Die Leitungen/Kabel übertragen die digitalen ISDN-Signale. Hinter der letzten ISDN-Anschlußdose wird der S₀-Bus mit einem Abschlußwiderstand terminiert. Der S₀ 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 S₀ 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 Software-Teil, 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 **X4000**. 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 remote 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 verschiedenen 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).
- 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** Internet-Zugang.

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

A	Abhörsicherung	370
	Access Lists	132, 349
	Activity Monitor	334
	ADSL	157
	Allgemeine PPP-Einstellungen	200
	allgemeine Sicherheitshinweise	31
	Allgemeine WAN-Einstellungen	194
	Arbeitsspeicher	380
	ARP	241
	Aufstellen und Anschließen	59
	Authentisierung	162, 200, 340
	Allgemeine Einstellungen	200
	TAF	368
	Auto-Logout	374
B	Backroute Verification	367
	Bandwidth on Demand	207
	Benutzer anlegen	142
	BinTec Companion CD	20
	BOOTP Relay Agent	275
	Boot-Sequenz	66
	BRICKware	20, 22, 113
	installieren	113
	Bridging	285
C	Callback	341
	CAPI	142
	Channel Bundling	205
	CHAP	162, 200, 340
	Checkliste für Sicherheitsfunktionen	376
	CLID	162, 339
	Closed User Group	343
	COM-Port-Treiber	116
	CompuServe	187
	Configuration Manager	78

Configuration Wizard	78, 109
Credits Based Accounting System	328
D	
Default-Route	162, 179
Delay after Connection Failure	204
Denial-of-Service-Attacke	374
Desktop-Gerät	37
DHCP-Server	129
Dienst	274, 349
Display	93
Display umstecken	55
Display-Schnittstelle	421
DNS	232, 254
Dokumentation	22
Domain Name	254
Dynamic IP Address Server	194
E	
Einbaugerät	40
Eingabetasten	93
Eingehende Rufe	
CAPI	142
ISDN-Login	142
Routing	142
Eingehende Rufnummer überprüfen	339
Einloggen	76, 338
Encryption	370
Enkapsulierung	162
Erweiterungskarten	53
Ein- und Ausbau	55
Extended Features Reference	22
Extended IP-Routing	368
F	
Feedbackmöglichkeit	29, 467
Fehlersituationen, typische	395
Festverbindungen	138, 151
Filter	132, 349, 363
Firewall	319

Firmennetzanbindung	162
Flash-Speicher	380
Fragebogen	467

G Garantiebedingungen	24
Grundgerät	36, 405
Desktopgerät	37
Einbaugerät	40
Schnittstellen	405
Technische Daten	405
Grundkonfiguration mit Setup Tool	119
Grundlegende IP-Einstellungen	249
Grundlegende Routereinstellungen	120

H Hardware	35
Aufstellen und Anschließen	59
Erweiterungskarten	53
Grundgerät	36
LEDs	63
Hinweise zur Initialkonfiguration	91
HTTP-Statusseite	332

I Internetzugang	162
Comuserve	187
T-Online	187
IP	
Grundlegende Einstellungen	249
Namensauflösung	254
Transit Network	229
IP-Adresse	
DHCP-Server	129
Eingeben mit MMI	93
Eingeben mit Setup Tool	126
IP Address Server	194
IP-Adreß-Pools	194
PCs im LAN	116
Pool	194

IPX	278
LAN-Schnittstelle	280
WAN-Partner	281
ISDN-B-Kanal	226
ISDN-BRI-Schnittstelle	
konfigurieren	138
Technische Daten	408
ISDN-Login	74, 142
J JAVA Statusmonitor	334
K Kanalbündelung	205
Kommandos	427
BRICKtools for Unix	435
SNMP-Shell	428
Kommunikationsanwendungen	116
Komprimierung	239
MS-STAC	239
STAC	239
Van Jacobson Header Compression	239
Van Jacobson Header Komprimierung	239
Konfiguration	118
Grundkonfiguration mit Configuration Wizard	109
Grundkonfiguration mit Setup Tool	119
Grundlegende Routereinstellungen	120
Hinweise zur Initialkonfiguration	91
Konfigurationsmanagement	379
PC einrichten	116
Sicherheitsfunktionen	319
sichern	191
Testen	118
Verteilung eingehender Rufe	142
Vorbereiten	111
WAN-Partner	162
WAN-Schnittstellen	138
Weiterführende Konfiguration mit Setup Tool	193
Konfigurationsdateien verwalten	380

	Konfigurationsmanagement	379
	Konfigurationsmöglichkeiten	78
	Konsolenschnittstelle	406
L	LAN-LAN-Kopplung	162
	LAN-Schnittstelle	
	ADSL-Zugang	157
	IPX	280
	konfigurieren	126
	Technische Daten	407
	Layer 1 Protocol	226
	Leased Lines	138, 151
	LEDs	63, 93
	Lieferumfang	18
	Lizenz	
	eintragen	121
	Zusatzlizenz	286
	Lizenzkarte	18
	Lokale Filter	363
M	Memory	380
	MIB	78
	MIB Reference	22
	MMI	
	Bedienung	93
	Display	93
	Display umstecken	55
	Eingabetasten	93
	IP-Adresse eingeben	93
	Netzmaske eingeben	93
	Statusinformationen	93
	Monitorfunktionen im Setup Tool	325
	MPPE	370
	MS-STAC	239
N	Namensauflösung	232
	NAT	185, 344

NetBIOS	232
NetBIOS-Filter	132
Network Address Translation	185, 344
Netzmaske	
Eingeben mit MMI	93
Eingeben mit Setup Tool	126
Netzteil	404
Novell-Netzwerke	278
P	
PAP	162, 200, 340
Paßwörter	76, 123
PC einrichten	116
Port	274
Ports	349
PPP-Authentisierung	162, 340
Allgemeine Einstellungen	200
PPP-Einstellungen	200
PPTP	373
Proxy ARP	241
R	
RAM	380
Regel	349
Release Notes	22
Remote-CAPI	116, 142, 343
RIP	236
Routing	162
Routing Information Protocol	236
Routing-Eintrag	162, 179
Rufnummern	
CAPI	142
ISDN-Login	142
Routing	142
RVS-COM Lite	116
S	
S0-Schnittstelle	
konfigurieren	138
Technische Daten	408

SAFERNET	319
Setup Tool	80
Bedienung	80
Grundkonfiguration	119
Menüstruktur	80
Monitorfunktionen	325
Weiterführende Konfiguration	193
Shorthold	162
Sicherheitsfunktionen	319
Abhörsicherung	370
Besonderheiten	374
Checkliste	376
Konfigurieren	319
Überwachen von Aktivitäten	320
Zugangssicherung	338
Sicherheitshinweise, allgemeine	31
Sichern der Konfiguration	191
SNMP-Shell	76, 78
Software Reference	22
Software-Update	388
STAC	239
Startup-Verhalten	374
Syslog-Messages	320
Systemdaten eintragen	123
Systemvoraussetzungen	23
Systemzeit	249
T TAF	368
Taschengeldkonto	328
T-DSL	157
Technische Daten	403
Grundgerät	405
Netzteil	404
Telnet	73
Time-Server	249
Token Authentication Firewall	368
T-Online	187

Transit Network	229
Troubleshooting	391
Hilfsmittel	392
IPX-Routing	399
ISDN-Verbindungen	396
Systemfehler	395
U Überwachen von Aktivitäten	320
Update	388
User Concept	142
V V.24-Schnittstelle	
Technische Daten	409
Van Jacobson Header Komprimierung	239
Verschlüsselung	370, 373
Verteilung eingehender Rufe	142
Virtual Private Network (VPN)	373
VPN	373
W WAN-Partner	
anlegen (Grundkonfiguration)	162
Beispiele	187
Compuserve	187
DNS	232
Enkapsulierung	162
Internetzugang	187
IPX	281
PPP-Authentisierung	162
Routing-Eintrag	162
Shorthold	162
T-Online	187
Transit Network	162
weiterführende Funktionen	204
WINS	232
WAN-Schnittstellen	138
Weiterführende Konfiguration mit Setup Tool	193
WINS	232, 254



X	X.21	151
	X.21-Schnittstelle	
	konfigurieren	151
	Technische Daten	409
	XIPR	368
Z	Zugangsmöglichkeiten	70
	Zugangssicherung	338
	Zurücksetzen in Auslieferungszustand	395
	Zusatzlizenz	286





Fragebogen zum Handbuch, FaxBack an 0911 - 9673 1498

Wie schätzen Sie Ihre eigenen Fähigkeiten ein?

- Netzwerkspezialist mittlere Netzwerk-
kenntnisse wenig Netzwerk-
kenntnisse

Wie beurteilen Sie den Umfang des Handbuchs?

- zu wenig genau richtig zu viel

Fehlt etwas Wichtiges im Handbuch?

- nein ja, und zwar:.....

Gibt es Überflüssiges im Handbuch?

- nein ja, und zwar:.....

Wie beurteilen Sie die Übersichtlichkeit des Handbuchs ?

- sehr gut gut mittel schlecht sehr schlecht

Wie beurteilen Sie die Verständlichkeit des Handbuchs (Beispiele, Erklärungen, Grafiken)?

- sehr gut gut mittel schlecht sehr schlecht

Hatten Sie beim Installieren/Konfigurieren ein Problem, das Sie mit dem Handbuch nicht lösen konnten?

- nein ja, und zwar:.....

Welche Konfigurationstools nutzen Sie?

- Configura- Setup Tool Configura- SNMP-Kom- andere:.....
tion Wizard tion Manager mandos

Kommentare:

.....
.....
.....
.....

