



X1000

Benutzerhandbuch


Installation und Konfiguration

Copyright © 2000 BinTec Communications AG, alle Rechte vorbehalten

Version 1.2

Dokument #70000N

November 2000



Ziel und Zweck Dieses Handbuch beschreibt die Installation und Erstkonfiguration von **X1000** mit Software Release 5.3.1. Für neueste Informationen und Hinweise zum aktuellen Software Release sollten Sie in jedem Fall zusätzlich unsere Release Note lesen – insbesondere, wenn Sie ein Software Update zu einem höheren Release-Stand durchführen. Die aktuellste Release Note ist immer zu finden unter www.bintec.de.

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

Die Informationen in diesem Handbuch können ohne Ankündigung geändert werden. Zusätzliche Informationen, sowie Änderungen und Release Notes für **X1000** finden Sie unter www.bintec.de.

Als ISDN-Multiprotokollrouter baut **X1000** in Abhängigkeit von der Systemkonfiguration ISDN-Verbindungen auf. Um ungewollte Gebühren zu vermeiden, sollten Sie das Produkt unbedingt überwachen. BinTec Communications AG übernimmt keine Verantwortung für Datenverlust, ungewollte Verbindungskosten und Schäden, die durch den unbeaufsichtigten Betrieb des Produkts entstanden sind.

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

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

Copyright 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 Normen **X1000** entspricht folgenden Richtlinien und 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-Richtlinien

Zulassungen:

- CE-Zulassungen

- TÜV/GS

- BAKOM-Zulassung (Schweiz)

Zusätzlich zu den CE-Richtlinien genügt **X1000** 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 Germany
Internet	www.bintec.de





Inhaltsverzeichnis	7
Willkommen!	13
Allgemeine Sicherheitshinweise	31
Los geht's	35
Grundlagen	89
Ein Draht zu X1000	111
Grundkonfiguration mit dem Setup Tool	135
Weiterführende Konfiguration	213
Sicherheitsmechanismen	307
Konfigurationsmanagement	369
Trouble Shooting	385
Technische Daten	395
Wichtige Kommandos	409
Glossar	419
Index	437



Inhaltsübersicht	5
Inhaltsverzeichnis	7
1 Willkommen!	13
1.1 Wozu X1000?	15
1.2 Lieferumfang	19
1.3 BinTec ISDN Companion CD	20
1.4 Dokumentation bei BinTec	22
1.5 Systemvoraussetzungen	23
1.6 Garantiebedingungen	24
1.7 Zu diesem Handbuch	26
1.7.1 Inhalt	26
1.7.2 Verwendung	28
2 Allgemeine Sicherheitshinweise	31
3 Los geht's	35
3.1 Aufstellen und Anschließen	37
3.2 Konfiguration vorbereiten	40
3.2.1 Daten sammeln	40
3.2.2 Was in Ihrem Windows-Netzwerk zu tun ist	43
3.3 BRICKware unter Windows installieren	47
3.4 Lösungsszenarien	49
3.4.1 Zugang zum Internet einrichten	49
3.4.2 Kommunikationsanwendungen nutzen	51
3.4.3 Eine Firmenniederlassung an die Firmenzentrale anbinden	52

3.4.4	Außendienstmitarbeitern ohne Router Zugang zur Firmenzentrale ermöglichen (Dial-in)	53
3.5	X1000 unter Windows konfigurieren	55
3.5.1	Router-Grundkonfiguration einrichten	58
3.5.2	Mit X1000 ins Internet	62
3.5.3	X1000 ans Firmennetz anbinden	64
3.5.4	Konfiguration abschließen	66
3.6	Remote-CAPI-Schnittstelle am PC	69
3.6.1	Remote CAPI Client auf allen weiteren PCs installieren	69
3.6.2	Remote CAPI konfigurieren	70
3.7	PC einrichten	71
3.7.1	Dem Rechner IP-Adresse, Gateway und DNS Server mitteilen	71
3.7.2	Die Rechner des Partnernetzes finden	73
3.8	Fax und Anrufbeantworter einrichten mit RVS-COM Lite	77
3.8.1	RVS-COM Lite installieren	77
3.8.2	RVS-COM Lite einrichten	80
3.9	Konfiguration testen	84
3.9.1	Internet-Zugang testen	84
3.9.2	E-Mails verschicken und empfangen	84
3.9.3	Ein Fax verschicken	84
3.9.4	Ein Fax empfangen	86
4	Grundlagen	89
4.1	ISDN-Grundlagen	90
4.2	Wenn es noch schneller gehen soll...	93
4.3	Dienste und Benutzer	94
4.4	X1000 als DHCP Server	98
4.5	Wie funktioniert Namensauflösung?	101
4.6	Was sind Routen und Default-Routen?	104

	4.7	Filter und NetBIOS	107
	4.8	MIB und SNMP	109
5	Ein Draht zu X1000		111
	5.1	Zugangsmöglichkeiten	112
	5.1.1	Zugang über die serielle Schnittstelle	113
	5.1.2	Zugang über LAN	115
	5.1.3	Zugang über ISDN	116
	5.2	Anmelden	118
	5.3	Konfigurationsmöglichkeiten	121
	5.3.1	Übersicht	121
	5.3.2	Bedienung und Menüstruktur des Setup Tools	122
6	Grundkonfiguration mit dem Setup Tool		135
	6.1	Grundlegende Router-Einstellungen	137
	6.1.1	Lizenzen eintragen	138
	6.1.2	Systemdaten eintragen	140
	6.1.3	LAN-Schnittstelle konfigurieren	143
	6.1.4	WAN-Schnittstelle konfigurieren	146
	6.1.5	X1000 als DHCP Server einrichten	159
	6.1.6	Filter setzen	162
	6.2	X1000 und das WAN	167
	6.2.1	WAN-Partner einrichten	169
	6.2.2	Mit X1000 ins Internet	195
	6.2.3	Ins Firmennetz einwählen	201
	6.3	Konfigurationsdatei sichern	211
7	Weiterführende Konfiguration		213
	7.1	Allgemeine WAN-Einstellungen	214
	7.1.1	Dynamic IP Address Server	214

7.1.2	CAPI User Concept	216
7.1.3	Allgemeine PPP-Einstellungen	220
7.1.4	X.31 TEI	222
7.2	WAN-Partner-spezifische Einstellungen	223
7.2.1	Delay after Connection Failure	223
7.2.2	Channel Bundling - Basiskonfiguration für Wählverbindungen	224
7.2.3	Channel Bundling - Bandwidth on Demand (BOD) - erweiterte Konfiguration für PPP-Verbindungen	226
7.2.4	Always On/Dynamic ISDN (AO/DI)	233
7.2.5	Layer 1 Protocol (ISDN-B-Kanal)	247
7.2.6	IP Transit Network	249
7.2.7	Übermittlung von DNS- und WINS-Server-IP-Adressen an WAN-Partner	253
7.2.8	Routing Information Protocol (RIP)	256
7.2.9	Komprimierung	259
7.2.10	Proxy ARP (Address Resolution Protocol)	261
7.2.11	Keepalive Monitoring	263
7.3	Grundlegende IP-Einstellungen	269
7.3.1	Systemzeit	269
7.3.2	Namensauflösung - X1000 mit DNS Proxy	273
7.3.3	Port-Nummern	294
7.3.4	BOOTP Relay Agent	295
7.4	IPX-Einstellungen	298
7.4.1	Allgemeine Einstellungen	298
7.4.2	LAN-Schnittstelle konfigurieren	300
7.4.3	WAN-Partner einrichten	301
7.5	Funktionen mit Zusatzlizenz	305
7.5.1	Virtual Private Network (VPN) und Verschlüsselung	305
7.5.2	IPSec (Internet Protocol Security)	305
7.5.3	Festverbindungen (leased lines)	305



8	Sicherheitsmechanismen	307
8.1	Überwachen von Aktivitäten	308
8.1.1	Syslog Messages	308
8.1.2	Monitorfunktionen im Setup Tool	313
8.1.3	Taschengeldkonto (Credits Based Accounting System)	317
8.1.4	HTTP-Statusseite	321
8.1.5	Activity Monitor	325
8.2	Zugangssicherung	328
8.2.1	Anmelden	328
8.2.2	Überprüfen der eingehenden Rufnummer	329
8.2.3	Authentisierung von PPP-Verbindungen mit PAP, CHAP oder MS-CHAP	330
8.2.4	Callback	330
8.2.5	Closed User Group	332
8.2.6	Zugriff auf Remote CAPI	332
8.2.7	NAT (Network Address Translation)	333
8.2.8	Filter (Access Lists)	338
8.2.9	Lokale Filter	352
8.2.10	Backroute Verification	356
8.2.11	TAF Client	357
8.2.12	Extended IP-Routing (XIPR)	357
8.3	Abhörsicherung	359
8.3.1	Verschlüsselung	359
8.3.2	VPN (mit Zusatzlizenz)	363
8.3.3	IPSec (mit Zusatzlizenz)	363
8.4	Besonderheiten	365
8.4.1	Startup-Verhalten	365
8.4.2	Autologout	365
8.4.3	Vorbeugung gegen Denial-of-Service-Attacken	365
8.5	Checkliste	367

9	Konfigurationsmanagement	369
9.1	Konfigurationsdateien verwalten	370
9.2	X1000 in den Auslieferungszustand versetzen	379
9.3	Software Update durchführen	381
10	Trouble Shooting	385
10.1	Hilfsmittel zum Trouble Shooting	386
10.1.1	Lokale SNMP-Shell-Kommandos	386
10.1.2	Externe Hilfsmittel	387
10.2	Typische Fehlersituationen	388
10.2.1	Systemfehler	388
10.2.2	ISDN-Verbindungen	389
10.2.3	IPX-Routing	392
11	Technische Daten	395
11.1	Allgemeine Produktmerkmale	396
11.2	LEDs auf der Vorderseite	399
11.3	Anschlüsse auf der Rückseite	402
11.4	Pin-Zuordnung	403
11.5	BOOT-Sequenz	406
12	Wichtige Kommandos	409
12.1	SNMP-Shell-Kommandos	410
12.2	BRICKtools for Unix Kommandos	417
	Glossar	419
	Index	437

1 Willkommen!

Wir dürfen Sie zum Kauf Ihres Personal Internet Access Routers von BinTec Communications AG beglückwünschen. Damit haben Sie einen Daten-Router der neuen Generation von BinTec Communications AG aus unserer Produktgruppe Personal Access erworben. Dieser leistungsstarke



Multiprotokoll-Router ermöglicht Ihnen die kostengünstige Vernetzung kleiner Netzwerke. **X1000** wird Ihnen in Zukunft die Anbindung Ihres Einzelarbeitsplatzes oder kleinen Unternehmens an das Internet und an andere Partnernetze (z. B. eine Firmenzentrale) ermöglichen. **X1000** wird Ihnen außerdem moderne Mittel der Bürokommunikation (Kommunikationsanwendungen wie z. B. Fax und Filetransfer) netzwerkweit an jedem Rechner verfügbar machen.

Wie geht's weiter?

Was Sie an X1000 haben...

..., was **X1000** für Sie bedeutet und was **X1000** alles kann, erfahren Sie auf den folgenden Seiten.

Wie Sie X1000 das Laufen lehren...

...erfahren Sie im [Kapitel 3, Seite 35](#). Dort zeigen wir Ihnen, wie Sie **X1000** innerhalb weniger Minuten von einem Windows-PC aus mit einem Konfigurationsassistenten in Betrieb nehmen und wie Sie weitere nützliche Hilfsprogramme installieren. Am Ende dieses Kapitels sind Sie in der Lage, im Internet zu surfen, E-Mails oder Faxe zu verschicken und zu empfangen und eine Verbindung mit einem Partnernetz herzustellen, um beispielsweise auf Daten einer Firmenzentrale zuzugreifen.

Was Sie sonst noch alles tun können...

...erklären wir ausführlich ab [Kapitel 6, Seite 135](#). Dort erfahren Sie alle Konfigurationsmöglichkeiten im Detail. Auch wenn Sie keinen Windows-PC haben, werden Sie dort schnelle Wege finden, **X1000** zu konfigurieren.

Wenn Sie bereits BinTec-Router konfiguriert haben... ..., Sie sich mit der Konfiguration gut auskennen und gleich loslegen wollen, fehlen Ihnen eigentlich nur noch der werkseitig eingestellte Benutzername und das Paßwort:

Benutzername	Paßwort
admin	bintec



Aber denken Sie daran, das Paßwort sofort zu ändern, wenn Sie sich das erste Mal auf **X1000** einloggen. Alle BinTec-Router werden mit gleichem Paßwort ausgeliefert. Sie sind daher erst gegen einen unauthorisierten Zugriff geschützt, wenn Sie das Paßwort ändern. Die Vorgehensweise bei der Änderung von Paßwörtern ist unter "[Paßwortänderung](#)", [Seite 128](#) beschrieben.

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

Pick-Up-Service Sollten jedoch einmal Probleme mit der Hardware von **X1000** auftreten, so bietet Ihnen BinTec Communications AG innerhalb eines Jahres einen kostenlosen Austausch Ihres defekten Geräts an. Nähere Information hierzu finden Sie in [Kapitel 1.6, Seite 24](#).

1.1 Wozu X1000?

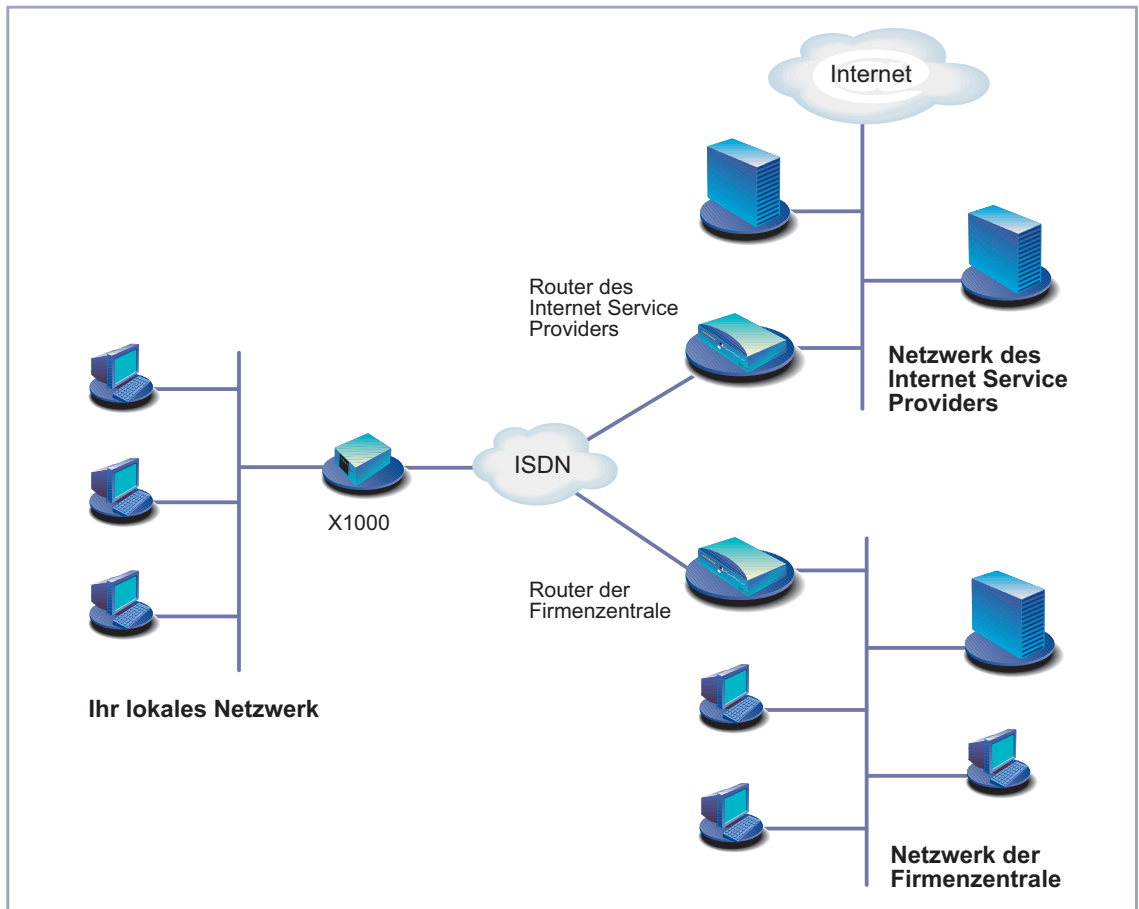


Bild 1-1: Grundszenario

Wozu Router wie X1000?

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

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

Wie aus vorheriger Abbildung ersichtlich ist, ist **X1000** für eine Verbindung der Netzwerke die entscheidende Komponente: Ihr Router ist die Verbindung zur Außenwelt. Jeder Router ist in der Abbildung über den ISDN-Anschluß an das ISDN gekoppelt und dient so als Bindeglied zwischen den einzelnen lokalen Netzwerken. Innerhalb jedes einzelnen Netzwerks (LAN) ist der Router wie ein normaler Rechner an das Netzwerk angeschlossen. Er hat die Aufgabe, gegebenenfalls Informationen aus dem eigenen Netz nach außen an ein anderes Netz (z. B. an das Netz Ihres Internet Service Providers oder das Netz einer Firmenzentrale) weiterzuleiten und dafür die geeigneten Wege (Routen) zu finden. Umgekehrt empfängt er Informationen und routet diese ins eigene Netz weiter.

Was kann **X1000**, was ISDN-Karten nicht könnten? Ihr **X1000** bietet weitaus mehr:

Ein Router für alle

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

Kommunikationsanwendungen

Für Kommunikationsanwendungen wie z. B. Anrufbeantworter, Fax, Dateitransfer und Eurofile-Transfer, die Sie von Ihrem Rechner aus bedienen, gilt das gleiche Prinzip wie beim Zugriff auf das Internet. Über eine BinTec-eigene Schnittstelle, die Remote CAPI, können alle Teilnehmer im LAN diese Dienste nutzen, dabei aber über **X1000** auf einen einzigen ISDN-Anschluß zugreifen. Voraussetzung ist, daß alle Teilnehmer eine geeignete Anwender-Software installiert haben, die die sogenannte CAPI-Schnittstelle unterstützt. Diese genormte Schnittstelle wird von den meisten Kommunikationsanwendungen verwendet. Im Lieferumfang von **X1000** ist eine entsprechende Software ent-

halten, RVS-COM Lite. Mit ihr decken Sie das Spektrum der gängigen Kommunikationsanwendungen ab.

Automatisches Einwählen und Beenden

Ein wesentlicher Vorteil von **X1000** zeigt sich außerdem in der Zugangsart. Ihr Router entscheidet – einmal konfiguriert – selbständig, ob und wie er eine Verbindung zum Internet Service Provider herstellen muß. Sie geben zum Beispiel in Ihren Browser eine externe WWW-Adresse ein, **X1000** stellt fest, daß die angeforderte Adresse außerhalb Ihres eigenen LANs liegt und baut die Verbindung zu Ihrem Internet Service Provider und somit dem Internet automatisch auf. Und – damit Sie Kosten sparen – beendet **X1000** die Verbindung nach einer definierten Zeit (Shorhold) wieder, wenn keine Informationen mehr ausgetauscht werden.

Das gleiche Prinzip wenden Sie an, um auf Daten eines anderen Standortes, z. B. Ihrer Firmenzentrale, bequem zuzugreifen. Sie können sogar unter Windows ein Netzlaufwerk mit einem Rechner der Firmenzentrale verbinden. Im Windows Explorer klicken Sie dann einfach auf das Symbol dieser Verknüpfung und "surfen" in den Verzeichnissen und Daten des entfernten Rechners wie auf Ihrer eigenen Festplatte. Um den Auf- und Abbau der Verbindung kümmert sich **X1000**.

Sicherheit

Auch bezüglich der Sicherheit bietet **X1000** einiges. Mit Ihrem Router besitzen Sie integrierte Firewall-Mechanismen. Ihr Router erfüllt alle Anforderungen bezüglich Zugangssicherheit umfangreich und kostengünstig. Er schirmt Ihr Netz gegen unbefugten Zugriff von außen ab. Dies wird möglich durch **X1000's** SAFERNET-Funktionen wie NAT, Verschlüsselung, Filter, Monitoring.

Konfiguration und Wartung

Für die Konfiguration von **X1000** bieten sich eine Reihe von Optionen. Die meisten Konfigurationsmethoden sind unabhängig vom Betriebssystem Ihres Rechners.

Die einfachste Methode unter Windows ist der Configuration Wizard. Dieser Konfigurationsassistent leitet Sie Schritt für Schritt durch die Konfiguration und unterstützt Sie, die wichtigsten Einstellungen an Ihrem Router vorzunehmen. In wenigen Minuten ist **X1000** einsatzbereit.

X1000 ist außerdem fernkonfigurier- und fernwartbar. Sobald Ihr Router – selbst im Auslieferungszustand – an das ISDN angeschlossen ist, können von einem anderen Standort aus (z. B. vom Administrator einer Firmenzentrale)

Konfigurationseinstellungen vorgenommen werden. Die Einrichtung des Systems können Sie so einem Verantwortlichen in der Zentrale überlassen.

Zusammenfassend Die Hauptvorteile von **X1000** sind:

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

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

1.2 Lieferumfang

X1000 wird zusammen mit folgenden Teilen ausgeliefert:

- Kabelsätze/Netzteil:
 - LAN-Kabel (RJ45, rot) für LAN-Anschluß an Hub
 - Adapterkabel (gekreuzt) zusammen mit rotem LAN-Kabel für LAN-Anschluß direkt an PC
 - ISDN-Kabel (RJ45, schwarz) für ISDN-Anschluß
 - Serielles Anschlußkabel (grau)
 - Steckernetzteil
- BinTec Companion CD
- Dokumentation:
 - Benutzerhandbuch
 - Kurzanleitung
 - Release Notes, falls erforderlich
- Zusätzliches Material:
 - Lizenzkarte mit Lizenzinformation

1.3 BinTec ISDN Companion CD

Auf Ihrer BinTec Companion CD finden Sie alle Programme, die Sie zur Installation, Konfiguration und Wartung von **X1000** brauchen.

- BRICKware**
- Der Configuration Wizard führt Sie Schritt für Schritt durch die Grundkonfiguration von **X1000**.
 - Der Activity Monitor ermöglicht es Ihnen, die Auslastung von **X1000** mit einem Blick zu überwachen.
 - Über das Terminal-Programm Gerät an COM1 bzw. Gerät an COM2 erhalten Sie Zugang zu **X1000** über die serielle Schnittstelle.
 - Remote CAPI Client
Mit dem Remote CAPI Client können Sie Kommunikationsanwendungen nutzen, die auf die genormte CAPI-Schnittstelle aufsetzen (z. B. RVS-COM Lite).
 - Token Authentication Firewall (TAF) Programm
Dieses Software-Paket benötigen Sie, wenn Sie das Sicherheitssystem von Security Dynamics verwenden.
 - Der Configuration Manager erlaubt es Ihnen, alle BinTec-Router im Netz über eine graphische Oberfläche zu konfigurieren und zu administrieren. Hier können Sie alle SNMP-Tabellen und -Variablen einsehen und bearbeiten.
 - Die DIME Tools dienen der Überwachung und Administration von **X1000**.

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

- RVS-COM Lite**
- Zusätzlich zur BRICKware ist auf Ihrer BinTec Companion CD das Kommunikationsprogramm RVS-COM Lite enthalten, das Ihnen typische Kommunikationsanwendungen wie z. B. Anrufbeantworter, Fax oder Dateitransfer auf Ihrem Rechner ermöglicht; wie, erklären wir in [Kapitel 3.8, Seite 77](#).



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](#))
- Gegebenenfalls eine Kopie der Router-Software (Auslieferungszustand)
- UNIX Tools (Administration)
- Adobe's Acrobat Reader
- MIB-Tabellen

1.4 Dokumentation bei BinTec

Die Dokumentation haben Sie zusammen mit **X1000** teilweise in gedruckter und komplett in elektronischer Form (PDF, HTML) erhalten. Die elektronischen Fassungen der verschiedenen Dokumente finden Sie auf Ihrer BinTec Companion CD. Zusätzlich zur Companion CD stehen alle Dokumente jeweils in der aktuellsten Version auf unserem WWW-Server unter www.bintec.de zum Download bereit. Es gibt:

- Benutzerhandbuch (gedruckt/PDF)
Dieses Handbuch.
- Faltblatt mit einer Kurzanleitung zur Erstkonfiguration von **X1000** (gedruckt/PDF)
- Referenzhandbücher (englisch, PDF/HTML)
 - Software Reference (PDF)
Online-Nachschlagewerk mit tiefergehenden Informationen zu hier beschriebenen Funktionen; Nachschlagewerk für zusätzliche, nur mit separater Lizenz verfügbare Funktionen (z. B. VPN); Nachschlagewerk für die internen SNMP-Tabellenstrukturen und die Bedienung der SNMP-Shell.
 - MIB Reference
HTML-Dokument mit Kurzbeschreibungen zu allen SNMP-Tabellen und Variablen von **X1000**.
- BRICKware for Windows (englisch, PDF)
Bedienungsanleitung für die Windows-Hilfsprogramme (BRICKware)
- Release Notes (meist englisch, PDF und/oder gedruckt)
Aktuelle Informationen und Hinweise zum aktuellen Software Release, Beschreibung aller Änderungen gegenüber dem vorherigen Release.
Im Dokument Release Note Logic finden Sie eine Anleitung zum Upgrade von BOOTmonitor und/oder Firmware Logic.
- UK Info (englisch, PDF)
Hinweise zum Betrieb von BinTec-Routern in Großbritannien.

1.5 Systemvoraussetzungen

X1000 können Sie von allen herkömmlichen Plattformen aus konfigurieren. Als Standalone-Gerät ist **X1000** 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.

Windows-PC Wenn Sie **X1000** mit einem Windows-PC konfigurieren möchten, benötigen Sie für die serielle Verbindung ein Terminal-Programm, z. B. **HyperTerminal**. Stellen Sie sicher, daß **HyperTerminal** bei der Windows-Installation auf dem PC mitinstalliert wurde.



Beachten Sie, daß bei Windows 98 und Windows ME **HyperTerminal** nicht in der Standardinstallation enthalten ist.

Configuration Wizard Speziell für die Verwendung des Configuration Wizard benötigen Sie:

- Rechner mit serieller Schnittstelle (V.24)
- Windows 95, Windows 98 oder Windows NT 4.0 bzw. Windows 2000
- Installierte Netzwerkkarte (10 MBit/s und/oder 100 MBit/s Ethernet)
- Installiertes Microsoft TCP/IP-Protokoll
Wie Sie herausfinden, ob Ihr Rechner über die nötigen Einstellungen verfügt und wie Sie gegebenenfalls die Einstellungen selbst vornehmen, erklären wir Ihnen, bevor Sie mit der Konfiguration loslegen.
- High Color Monitor (mehr als 256 Farben) für die korrekte Darstellung der Grafiken

Remote CAPI Die CAPI-Unterstützung für Kommunikationsapplikationen und Unified Messaging steht Ihnen für folgende Systeme zur Verfügung:

- Windows 95, Windows 98 bzw. Windows 2000 oder Windows NT 4.0
- Novell Netware 3.1x, 4.0x und 5.x

1.6 Garantiebedingungen

X1000 hat 24 Monate Garantie ab Kaufdatum.

Verlängern Sie die Garantiezeit für Ihren **X1000** kostenlos auf 6 Jahre!

Wie?

Registrieren Sie sich einfach innerhalb von 14 Tagen ab Kaufdatum online als BinTec **X1000** Kunde unter www.bintec.de/X1000/.

Für Ihre Bemühungen erhalten Sie von uns eine Garantieverlängerung von 2 auf 6 Jahre und ein kleines Dankeschön.

- Garantie**
1. Hiermit garantiert BinTec, daß dieses Gerät vom Zeitpunkt des Ersterwerbs für einen Zeitraum von 24 Monaten keine Material- und Verarbeitungsfehler aufweist. Sollten während der Garantiezeit Mängel am Gerät auftreten, die auf Material- oder Verarbeitungsfehlern beruhen, wird BinTec das Gerät nach den folgenden Bedingungen ohne Berechnung der Arbeits- und Materialkosten reparieren oder (nach Ermessen von BinTec) das Gerät selbst oder seine schadhaften Teile ersetzen. Austauschgeräte oder -teile gehen in das Eigentum von BinTec über. Für Austauschgeräte oder Ersatzteile gilt die verbleibende ursprüngliche Garantiezeit, mindestens jedoch eine Garantiezeit von 6 (sechs) Monaten vom Zeitpunkt der Reparatur oder des Austausches.
 2. Garantieleistungen werden nur erbracht, wenn die Originalrechnung bzw. der Kassenbeleg (unter Angabe von Kaufdatum, Produkttyp und Name des Händlers) und eine Fehlerbeschreibung zusammen mit dem defekten Gerät vorgelegt werden.
 3. Vor der Inanspruchnahme von Garantieleistungen sichern Sie unbedingt Ihre Konfiguration. BinTec haftet nicht für den Verlust dieser Daten. Bevor Sie das Gerät über Ihren Händler zur Reparatur zurücksenden, entfernen Sie bitte alle Teile, Funktionen, Ausstattungen, Veränderungen und Zusatzgeräte, die nicht unter die Garantie fallen. BinTec haftet nicht für Beschädigung oder Verlust dieser Teile oder Vorrichtungen. Für Änderungen, Löschungen oder andere Modifikationen in der Konfiguration des Gerätes haftet BinTec nicht. Das Gerät wird Ihnen mit einem aktuellen Softwarestand, unkonfiguriert zurückgegeben.

4. Diese Garantie umfaßt keinen der folgenden Punkte
 - (1) Regelmäßige Wartung und Reparatur oder Ersatz von Teilen bedingt durch normalen Verschleiß;
 - (2) Mit diesem Gerät gelieferte Verbrauchsmittel
 - (3) Beseitigung von Gebrauchsspuren
 - (4) Beschädigung oder Verlust von Konfigurationsdaten
 - (5) Schäden, die verursacht sind durch (a) höhere Gewalt oder Gründe, die außerhalb des Einflußbereiches von BinTec liegen; (b) unsachgemäßen Gebrauch, insbesondere den Gebrauch des Gerätes zu einem anderen als dem vorgesehenen Zweck oder den Gebrauch unter Nichtbeachtung der Bedienungs- und Wartungsanleitung von BinTec; (c) unsachgemäße Verwendung oder Wartung des Gerätes; (d) Anschluß des Gerätes an ungeeignete Stromquellen; (e) physikalische Beschädigung des Gehäuses; (f) Reparaturversuche durch nicht von BinTec autorisierte Dritte; (g) Einsatz des Gerätes mit Zubehör, Geräten oder Zusatzausrüstungen Dritter, nicht von BinTec autorisierter, Hersteller.
5. Kann BinTec nachweisen, daß kein Gewährleistungsfall vorliegt, so gehen die Aufwendungen für die Fehlersuche sowie für die weiteren Leistungen, die damit im Zusammenhang stehen, zu Lasten des Kunden.
6. Diese Garantie gilt nicht, wenn die Typen- oder Seriennummer des Gerätes geändert, gelöscht, entfernt oder unleserlich gemacht wurde.

Pick-Up-Service Abgesehen von der gewährten Garantie bietet Ihnen BinTec Communications AG einen Pick Up Service für **X1000**: Sollten innerhalb eines Jahres Probleme bei der Hardware des Geräts auftreten, so können Sie **X1000** kostenlos ersetzen lassen. Ihr defektes Gerät wird in der Regel am nächsten Arbeitstag bei Ihnen abgeholt und es wird Ihnen gleichzeitig ein Austauschgerät zugestellt.

Um Ihnen die Inanspruchnahme unseres Pick Up Service zu erleichtern, finden Sie ein Formular zur Erteilung des Auftrags Ihrem Gerät beige packt bzw. im World Wide Web unter www.bintec.de.

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.
3: "Los geht's"	Anweisungen, wie Sie X1000 mit dem Configuration Wizard in wenigen Minuten in Betrieb nehmen und wie Sie weitere nützliche Software installieren und einrichten.
4: "Grundlagen"	Wichtige Grundlagen zum Thema Router und Netzwerke.
5: "Ein Draht zu X1000"	Grundlagen zum Umgang mit dem Setup Tool.
6: "Grundkonfiguration mit dem Setup Tool"	Wie Sie X1000 mit dem Setup Tool (alternativ zum Configuration Wizard) in Betrieb nehmen.
7: "Weiterführende Konfiguration"	Wie Sie weitere Konfigurationseinstellungen mit dem Setup Tool vornehmen.
8: "Sicherheitsmechanismen"	Wie Sie Sicherheitsmechanismen gemäß SAFERNET einrichten, z. B. NAT (Network Address Translation) oder CLID (Calling Line Identification).
9: "Konfigurationsmanagement"	Wie Sie Konfigurationsdateien verwalten und wie Sie Software Updates durchführen.
10: "Trouble Shooting"	Wichtige Hinweise zur Fehlerbehebung.
11: "Technische Daten"	Die technischen Daten von X1000 .

Kapitel	Inhalt
12: "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 zusätzliches Hintergrundwissen erläutert wird.
	<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	Kennzeichnet Menüs und Untermenüs im Setup Tool.
nicht-proportional (Courier), z. B. ping 192.168.1.254	<ul style="list-style-type: none"> ■ Kennzeichnet Kommandos (z. B. in der SNMP-Shell), die Sie wie dargestellt eingeben müssen. ■ Darstellung im Setup Tool.
<IP Adresse>	Kennzeichnet Eingaben, bei denen Sie den in Klammern gesetzten Ausdruck durch Ihren Wert ersetzen. Die spitzen Klammern fallen bei der Eingabe weg.
fett, kursiv, z. B. BigBoss	Kennzeichnet Beispielbegriffe.
fett, z. B. ➤➤ MIB	Kennzeichnet Begriffe, die Sie im Glossar finden (Online ist der Doppelpfeil klickbar).
fett, z. B. biboAdmLoginTable, Windows-Startmenü	<ul style="list-style-type: none"> ■ Kennzeichnet Felder im Setup Tool und MIB-Tabellen/-Variablen. ■ Kennzeichnet Tasten, Tastenkombinationen und Windows-Begriffe.
<i>kursiv, z. B. none</i>	Kennzeichnet Werte, die Sie im Setup Tool oder bei MIB-Variablen eintragen bzw. die eingestellt werden können.
Online: blau	Kennzeichnung von Links.

Tabelle 1-3: Auszeichnungselemente

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 **X1000** 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 **X1000** die Hinweise für die Umgebungsbedingungen (vgl. Technische Daten). Verwenden Sie eine feste und ebene Unterlage.
 - Wenn das Gerät aus kalter Umgebung in den Betriebsraum gebracht wird, kann Betauung sowohl am Geräteäußeren als auch im Geräteinneren auftreten. Warten Sie, bis Ihr Gerät temperaturangepasst und absolut trocken ist, bevor Sie es in Betrieb nehmen. Beachten Sie die Umweltbedingungen in den Technischen Daten.
 - Überprüfen Sie, ob die auf dem Typenschild des Netzteils angegebene Nennspannung mit der örtlichen Netzspannung übereinstimmt. **X1000** darf nur mit dem original BinTec-Steckernetzteil (5 V DC) betrieben werden. BinTec Communications AG haftet nicht für Schäden, die durch die Verwendung eines anderen Steckernetzteils hervorgerufen werden.
 - Beachten Sie beim Verkabeln die Reihenfolge, wie im Handbuch beschrieben. Verkabeln Sie zuerst LAN-, ISDN- und serielle Anschlüsse, schließen Sie dann die Stromversorgung an, und schalten Sie zum Schluß **X1000** ein.
 - Überprüfen Sie, ob Sie die Verkabelung – insbesondere die ISDN- und LAN-Verkabelung – richtig durchgeführt haben, bevor Sie **X1000** in Betrieb nehmen. Der ISDN-Anschluß von **X1000** darf nicht mit dem Ethernet-Anschluß Ihres Rechners oder Hubs verbunden werden, der LAN-Anschluß von **X1000** nicht mit Ihrem ISDN-Anschluß.
 - Verwenden Sie für die Verkabelung nur die beigelegten Kabel. Falls Sie andere Kabel verwenden, übernimmt BinTec Communications AG für auftretende Schäden oder Beeinträchtigung der Funktionalität keine Haftung.

- Verlegen Sie Leitungen so, daß sie keine Gefahrenquelle (Stolpergefahr) bilden und nicht beschädigt werden.
 - Schließen Sie Datenübertragungsleitungen während eines Gewitters weder an noch ziehen Sie sie ab oder berühren Sie diese.
- Bestimmungsgemäße Verwendung, Betrieb**
- **X1000** ist für den Einsatz in einer Büroumgebung bestimmt. Als Multiprotokoll-Router baut **X1000** in Abhängigkeit von der Systemkonfiguration WAN-Verbindungen auf. Um ungewollte Gebühren zu vermeiden, sollten Sie das Produkt unbedingt überwachen.
 - **X1000** entspricht den einschlägigen Sicherheitsbestimmungen für Einrichtungen der Informationstechnik für den Einsatz in einer Büroumgebung.
 - Der bestimmungsgemäße Betrieb gemäß IEC 950/EN 60950 des Systems ist nur bei montiertem Gehäusedeckel gewährleistet (Kühlung, Brandschutz, Funkentstörung).
 - Die Umgebungstemperatur sollte 50°C nicht übersteigen. Vermeiden Sie direkte Sonneneinstrahlung.
 - Achten Sie darauf, daß keine Gegenstände (z. B. Büroklammern) oder Flüssigkeiten ins Innere des Geräts gelangen (elektrischer Schlag, Kurzschluß). Achten Sie auf ausreichende Kühlung.
 - Unterbrechen Sie in Notfällen (z. B. beschädigtes Gehäuse oder Bedienelement, Eindringen von Flüssigkeit oder Fremdkörpern) sofort die Stromversorgung und verständigen Sie den Service.
- Reinigung und Reparatur**
- Das Gerät darf nur durch geschultes Fachpersonal geöffnet werden. Lassen Sie daher Reparaturen am Gerät nur von einer BinTec-autorisierten Servicestelle durchführen. Wo sich die Servicestelle befindet, erfahren Sie von Ihrem Händler. Durch unbefugtes Öffnen und unsachgemäße Reparaturen können erhebliche Gefahren für den Benutzer entstehen (z. B. Stromschlag). Unerlaubtes Öffnen der Geräte hat den Garantie- und Haftungsausschluß der BinTec Communications AG zur Folge.
 - Das Gerät darf auf keinen Fall naß gereinigt werden. Durch eindringendes Wasser können erhebliche Gefahren für den Benutzer (z. B. Stromschlag) und erhebliche Schäden am Gerät entstehen.

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

3 Los geht's

Dieses Kapitel hilft Ihnen, so schnell wie möglich die wichtigsten und gängigen Anwendungen für Ihr lokales Netzwerk oder Ihren Einzelarbeitsplatz zu konfigurieren. Um Ihnen die Konfiguration so einfach wie möglich zu machen, unterstützt Sie ein Konfigurationsassistent, Ihr **Configuration Wizard**. Mit Ihm haben Sie **X1000** in wenigen Minuten konfiguriert.



Am Ende dieses Kapitels können Sie:

- **X1000** im LAN erreichen
- Im Internet surfen
- Faxe verschicken und empfangen
- Bei Bedarf eine Verbindung mit einem entfernten Netzwerk herstellen (LAN-LAN-Kopplung, z. B. Ihre Firmenzentrale), um bequem von zu Hause aus auf Daten der Zentrale zuzugreifen.

Um diese Anwendungen einzurichten, müssen Sie:

- **X1000** zunächst aufstellen und anschließen ([Kapitel 3.1, Seite 37](#))
- Einige Vorbereitungen treffen ([Kapitel 3.2, Seite 40](#))
- Windows-Software installieren und einrichten:
 - BRICKware for Windows installieren ([Kapitel 3.3, Seite 47](#))
 - **X1000** mit dem Configuration Wizard konfigurieren ([Kapitel 3.5, Seite 55](#))
 - Remote CAPI-Schnittstelle konfigurieren ([Kapitel 3.6, Seite 69](#))
- Eventuell zusätzliche Einstellungen an Ihren Rechnern vornehmen ([Kapitel 3.7, Seite 71](#))
- RVS-COM Lite installieren und einrichten ([Kapitel 3.8, Seite 77](#))

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



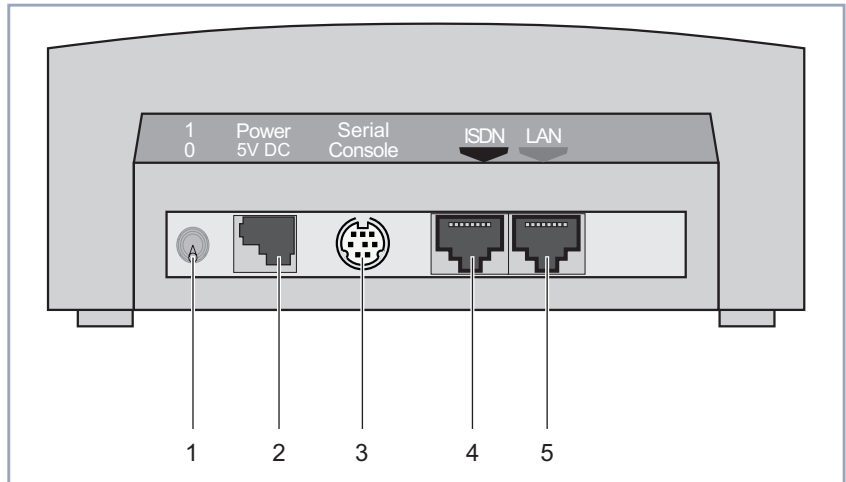
Wie Sie Ihre Konfiguration nach Abschluß der Grundkonfiguration optimieren können, finden Sie ab [Kapitel 7, Seite 213](#).

Wenn Sie sich fragen, wie Sie Ihre Grundkonfiguration ohne den Configuration Wizard einrichten (z. B. weil Sie kein Windows-Betriebssystem verwenden), lesen Sie [Kapitel 6, Seite 135](#).



Dieses Kapitel hält Sie nicht unnötig mit technischen Details von einer raschen Konfiguration ab. Wenn Sie aber später trotzdem einige Hintergrundinformationen wissen wollen, dann lesen Sie [Kapitel 4, Seite 89](#).

3.1 Aufstellen und Anschließen



1	Ein-/Ausschalter	4	ISDN-S ₀ -Schnittstelle
2	Stromversorgungsanschluß	5	LAN-Schnittstelle (10/100 Base-T Ethernet), am Gerät rot gekennzeichnet
3	Serielle Schnittstelle		

Bild 3-1: **X1000** Rückansicht



X1000 können Sie wahlweise an die Netzwerkkarte Ihres Rechners oder an einen Hub anschließen, wenn Sie ein kleines Netzwerk besitzen. Sie müssen lediglich auf die Wahl der Kabel achten.



Über den ISDN-Anschluß (4) verbinden Sie **X1000** mit dem ISDN. Ob Sie eine ISDN-Anschlußdose, einen ►► **NTBA-Adapter** oder eine TK-Anlage verwenden, macht für **X1000** keinen Unterschied. Wollen Sie jedoch TK-Anlagen-spezifische Funktionen nutzen, schließen Sie **X1000** an die TK-Anlage an. So können Sie z. B. Rufnummern sperren, die dann bei **X1000** gar nicht erst ankommen. Oder Sie kontrollieren die Gebühren der Rufnummern, die Sie **X1000** zuweisen.



Achtung!

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

- Verwenden Sie ausschließlich das mitgelieferte Steckernetzteil (5 V DC).
- Vergewissern Sie sich, daß die auf dem Steckernetzteil vermerkte Nennspannung mit der lokalen Spannungsversorgung übereinstimmt.



Achtung!

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

- Verbinden Sie immer nur die LAN-Schnittstelle von **X1000** mit der LAN-Schnittstelle des Rechners/Hubs und die ISDN-Schnittstelle von **X1000** mit dem ISDN-Anschluß.

Gehen Sie beim Anschließen in folgender Reihenfolge vor:

- Stellen Sie **X1000** auf eine feste, ebene Unterlage.
- Verbinden Sie die serielle Schnittstelle Ihres Rechners (COM1 oder COM2) mit der seriellen Schnittstelle des Routers (3, vgl. [Bild 3-1, Seite 37](#)). Verwenden Sie dazu das mitgelieferte serielle (graue) Kabel.

Sie können **X1000** entweder mit Ihrem Hub (LAN) oder mit der Netzwerkkarte Ihres Rechners (Einzelarbeitsplatz) verbinden.

Um **X1000** an Ihr LAN anzuschließen, benötigen Sie das mitgelieferte rote LAN-Kabel.

- Verbinden Sie die rot gekennzeichnete LAN-Schnittstelle von **X1000** (5) mit Ihrem LAN.
Die Geschwindigkeit Ihres LAN (10 MBit/s oder 100 MBit/s) wird automatisch erkannt (autosensing).

Wenn Sie **X1000** nicht an ein LAN anschließen, sondern direkt mit der Netzwerkkarte Ihres Rechners verbinden wollen (Einzelarbeitsplatz), benötigen Sie zusätzlich zum roten LAN-Kabel das Adapterkabel.

- Verbinden Sie die LAN-Schnittstelle von **X1000** mit Ihrem Rechner. Verbinden Sie dazu das rote LAN-Kabel mit der rot gekennzeichneten LAN-Schnittstelle von **X1000** (5). Stecken Sie das Adapterkabel an das rote Kabel. Verbinden Sie das Adapterkabel mit der Netzwerkkarte Ihres Rechners.
- Verbinden Sie die ISDN-Schnittstelle des Routers (4) über das mitgelieferte schwarze ISDN-Kabel (RJ45) mit Ihrem ISDN-Anschluß.



Wenn Sie für den Anschluß des Modems von der Deutschen Telekom AG oder einem anderen Provider ein spezielles Kabel erhalten haben, so verwenden Sie ausschließlich dieses mitgelieferte Kabel. Zur Verlängerung des Kabels verwenden Sie gegebenenfalls ein Standard-Ethernet-Kabel.

- Schließen Sie **X1000** über den Stromversorgungsanschluß (2) mit dem mitgelieferten Netzadapter an eine Steckdose an.
- Schalten Sie den Router mit dem Ein-/Ausschalter (1) ein.
X1000 führt einen Selbsttest durch. Wenn Sie alle Kabel richtig angeschlossen haben, erlischt die rote LED ERR am Ende des Selbsttests; die grüne LED PWR (Betriebsanzeige) leuchtet.

3.2 Konfiguration vorbereiten

3.2.1 Daten sammeln

Bevor Sie gleich mit der Konfiguration loslegen, sollten Sie Daten für folgende Zwecke bereitlegen – je nachdem, was Sie mit **X1000** machen wollen:

- Router-Grundkonfiguration mit Lizenzierung (obligatorisch)
- Internet-Zugang (optional)
- Firmennetzanbindung (optional)

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

Router-Grundkonfiguration

Für eine Grundkonfiguration von **X1000** benötigen Sie Informationen, die Ihren ISDN-Anschluß und Ihre Netzwerkumgebung betreffen:

Zugangsdaten	Beispielwert	Ihre Werte
ISDN-Rufnummern	967310	
Die ISDN-Rufnummern erhalten Sie mit Ihrem ISDN-Anschluß.	967311 967312	
X1000 IP-Adresse	192.168.1.254	
X1000 Netzmaske	255.255.255.0	



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



Im folgenden beschreiben wir die Einstellungen für den Anschluß von **X1000** am NTBA-Adapter. Beim Anschluß an eine TK-Anlage beachten Sie die Besonderheiten Ihres Anschlusses und lesen Sie gegebenenfalls in der Dokumentation Ihrer TK-Anlage nach.



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

Lizenzkarte Für die Grundkonfiguration brauchen Sie schließlich nur noch Ihre Lizenzkarte. Diese haben Sie zusammen mit **X1000** erhalten. Auf der Karte sind Seriennummer, Maske und Key angegeben, die Sie für eine Freischaltung der Funktionen von **X1000** benötigen. Auf der Lizenzkarte befindet sich auch die Lizenznummer für das Kommunikationsprogramm RVS-COM Lite.

Internet-Zugang Wenn Sie einen Internet-Zugang einrichten wollen, brauchen Sie einen Internet Service Provider (kurz ISP). Daran haben Sie wahrscheinlich schon gedacht. Wenn nicht, sollten Sie das in den nächsten Tagen nachholen oder einen Anschluß "Internet by call" benutzen (siehe nächster Absatz). Von Ihrem ISP bekommen Sie Ihre persönlichen Zugangsdaten mitgeteilt. Die Bezeichnungen der benötigten Zugangsdaten können unter Umständen von ISP zu ISP leicht variieren. Grundsätzlich jedoch handelt es sich um die gleiche Art von Information, die Sie zur Einwahl und Festlegung Ihres persönlichen Internet-Zugangs benötigen. In der nachfolgenden Tabelle sind die Zugangsdaten zusammengestellt, die auch **X1000** für eine Verbindung zum Internet benötigt.

Zugangsdaten	Beispielwert	Ihre Werte
Providername	<i>GoInternet</i>	
Einwahlnummer Die ISDN-Rufnummer, unter der Sie sich beim Internet Service Provider einwählen.	<i>1234567</i>	
Anschlußkennung Ihr Benutzername	<i>MyName</i>	
Paßwort	<i>TopSecret</i>	



Wenn **X1000** an eine TK-Anlage angeschlossen ist, bei der für eine Amtsholung eine führende "0" gewählt wird, müssen Sie diese führende Null bei der Einwahlnummer berücksichtigen.

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

Zugangsdaten	Beispielwert	Ihre Werte
T-Online-Nummer	081512345678	
Mitbenutzerkennung	0001	



Darüber hinaus bieten einige ISPs die Möglichkeit, auf das Internet zuzugreifen, ohne sich vorher anzumelden (sogenanntes "Internet by call"). So können Sie sofort testen, ob Ihr Internet-Zugang mit **X1000** funktioniert, auch wenn Sie später Ihre persönlichen Zugangsdaten bei einem anderen ISP beantragen möchten.

Firmennetzanbindung

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

Vor jeder Verbindung prüfen **X1000** und der Router Ihrer Firmenzentrale, ob sie den Ruf des Partners entgegennehmen. Die Rufannahme geschieht nur bei korrekter Authentisierung, um das Netz vor unbefugtem Zugriff zu schützen. Die Authentisierung erfolgt anhand des gemeinsamen Paßwortes und anhand von zwei Kennungen, die Sie und auch Ihr Partner für die Verbindung verwenden.

Zugangsdaten	Beispielwert	Ihre Wert
Partnername Kennung der Firmenzentrale	BigBoss	
Einwahlnummer Rufnummer des Routers der Firmenzentrale	0911987654321	

Zugangsdaten	Beispielwert	Ihre Wert
Lokaler Name Ihre eigene Kennung. Diesen Namen muß der Partner (Ihre Firmenzentrale) bei seinem Router als Partnernamen eintragen.	<i>LittleIndian</i>	
Paßwort Gemeinsames Paßwort für diese Verbindung	<i>Secret</i>	
Netzadresse(n) der Firmenzentrale	<i>10.1.1.0</i>	
Netzmaske(n) der Firmenzentrale	<i>255.255.255.0</i>	



Wie Sie weitere Sicherheitsmechanismen anwenden, z. B. Authentisierung anhand der Rufnummer (CLID) oder Verbergen des eigenen Netzes nach außen (NAT), erklärt Ihnen [Kapitel 8, Seite 307](#).



Wenn **X1000** an eine TK-Anlage angeschlossen ist, bei der für eine Amtsholung eine führende "0" gewählt wird, müssen Sie diese führende Null bei der Einwahlnummer berücksichtigen.



Netzadresse und Netzmaske des WAN-Partners (Firmenzentrale) brauchen Sie nur, wenn Sie zusätzlich zur LAN-LAN-Kopplung einen Internet-Zugang einrichten. Wenn Sie keinen Internet-Zugang einrichten, wird **X1000** so konfiguriert, daß automatisch alle Daten zum WAN-Partner geleitet werden, die nicht für das eigene Netz bestimmt sind (Default-Route).

3.2.2 Was in Ihrem Windows-Netzwerk zu tun ist

Nun haben Sie alle Daten gesammelt, die **X1000** wissen muß.

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

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

TCP/IP-Protokoll prüfen

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

- Windows 95/98**
- Klicken Sie im Windows-Startmenü auf **Einstellungen** ➤ **Systemsteuerung**.
 - Doppelklicken Sie auf **Netzwerk**.
 - Suchen Sie in der Liste der Netzwerkkomponenten **TCP/IP**.
 - Wenn Sie den Eintrag nicht finden, installieren Sie das TCP/IP-Protokoll wie unten beschrieben.
- Windows NT**
- Klicken Sie im Windows-Startmenü auf **Einstellungen** ➤ **Systemsteuerung**.
 - Doppelklicken Sie auf **Netzwerk**.
 - Wählen Sie das Register **Protokolle** und suchen Sie in der Liste der Netzwerkkomponenten **TCP/IP-Protokoll**.
 - Wenn Sie den Eintrag nicht finden, installieren Sie das TCP/IP-Protokoll wie unten beschrieben.
- Windows 2000**
- Klicken Sie im Windows-Startmenü auf **Einstellungen** ➤ **Netzwerk- und DFÜ-Verbindungen**.
 - Doppelklicken Sie auf **LAN-Verbindung**.
 - Klicken Sie im Register **Allgemein** auf **Eigenschaften**. Suchen Sie in der Liste der Netzwerkkomponenten **Internetprotokoll (TCP/IP)**.

- Wenn Sie den Eintrag nicht finden, installieren Sie das TCP/IP-Protokoll wie unten beschrieben.

TCP/IP-Protokoll installieren

- Windows 95/98**
- Klicken Sie im Dialogfenster **Netzwerk** auf **Hinzufügen**.
 - Wählen Sie in der Liste der Netzwerkkomponenten **Protokoll** und klicken Sie auf **Hinzufügen**.
 - Wählen Sie als Hersteller **Microsoft** und als Netzwerkprotokoll **TCP/IP** und klicken Sie auf **OK**.
 - Wenn Sie ein bestehendes Netzwerk haben, müssen Sie an dieser Stelle eventuell weitere Einstellungen vornehmen. Fragen Sie Ihren Systemadministrator.
 - Wenn Sie ein neues Netzwerk einrichten, klicken Sie auf **OK**.
 - Folgen Sie den Anweisungen am Bildschirm und starten Sie zum Schluß den Rechner neu.
 - Wiederholen Sie die Installation für alle Rechner im Netz.
- Windows NT**
- Klicken Sie im Dialogfenster **Netzwerk** auf das Register **Protokolle**. Klicken Sie auf **Hinzufügen**.
 - Wählen Sie in der Liste der Netzwerkprotokolle **TCP/IP-Protokoll**. Klicken Sie auf **OK**.
 - Wenn Sie ein neues Netzwerk einrichten, bestätigen Sie die Frage mit **Ja**.
 - Bei einem bestehenden Netzwerk fragen Sie Ihren Systemadministrator.
 - Folgen Sie den Anweisungen am Bildschirm und starten Sie zum Schluß den Rechner neu.
- Windows 2000**
- Klicken Sie im Windows-Startmenü auf **Einstellungen** ➤ **Netzwerk- und DFÜ-Verbindungen**.
 - Doppelklicken Sie auf **LAN-Verbindung**.
 - Klicken Sie im Register **Allgemein** auf **Eigenschaften**.
 - Wählen Sie das Register **Allgemein** und klicken Sie auf **Installieren**.
 - Wählen Sie in der Liste der Netzwerkkomponenten **Protokoll** und klicken Sie auf **Hinzufügen**.

- Wählen Sie als Netzwerkprotokoll **Internetprotokoll (TCP/IP)** und klicken Sie auf **OK**.
- Wenn Sie ein bestehendes Netzwerk haben, müssen Sie an dieser Stelle eventuell weitere Einstellungen vornehmen. Fragen Sie Ihren Systemadministrator.
- Wenn Sie ein neues Netzwerk einrichten, klicken Sie auf **OK** und auf **Schließen**.
- Folgen Sie den Anweisungen am Bildschirm und starten Sie zum Schluß den Rechner neu.

Abschließend ➤ Wiederholen Sie die Installation für alle Rechner im Netz, wenn Sie dort LAN-LAN-Kopplung, Internet-Zugang oder Kommunikationsanwendungen über **X1000** nutzen wollen.

3.3 BRICKware unter Windows installieren

- Schließen Sie alle Windows-Programme auf Ihrem PC.
- Legen Sie Ihre BinTec Companion CD in das CD-ROM-Laufwerk Ihres PCs ein.
Nach kurzer Zeit erscheint automatisch das Startfenster.
- Wenn das Startfenster nicht automatisch erscheint, klicken Sie im Windows Explorer auf Ihr CD-ROM-Laufwerk und doppelklicken Sie auf **setup.exe**. (Oder klicken Sie auf **Einstellungen** ➤ **Systemsteuerung**. Klicken Sie erst auf **Software** und dann auf **Installieren**. Folgen Sie den Anweisungen auf dem Bildschirm.)
- Wählen Sie im Startfenster die gewünschte Sprache aus bzw. belassen Sie gegebenenfalls die Voreinstellung.
- Wählen Sie *BRICKware* aus.
Der Installationsassistent wird aufgerufen.

Falls Sie auf Ihrem PC eine Version von BRICKware gespeichert haben, die älter als Version 5.2.1 ist, werden Sie aufgefordert, diese zu deinstallieren, um danach die aktuelle Version der BRICKware zu installieren.

Ab Version 5.2.1 können Sie ein Update auf Ihre BRICKware durchführen. Falls Sie die aktuelle Version von BRICKware bereits auf Ihrem Rechner gespeichert haben, können Sie während einer erneuten Installation unter verschiedenen Installationsmöglichkeiten wählen.

Deinstallieren Wenn Sie aufgefordert werden, BRICKware zu deinstallieren, folgen Sie den Anweisungen auf dem Bildschirm, um das Programm von Ihrem PC zu entfernen. Vor dem Deinstallieren wird die Datei win.ini auf Ihrem PC gesichert.

Ein Meldungsfenster informiert Sie, sobald BRICKware deinstalliert ist, Sie können die Software jetzt neu installieren.

Neuinstallation Gehen Sie folgendermaßen vor, um BRICKware zu installieren

- Klicken Sie auf **Weiter**.
- Geben Sie den Zielordner an, in den BRICKware installiert werden soll bzw. übernehmen Sie die Voreinstellung.
- Klicken Sie auf **Weiter**.

- Wählen Sie Ihren Routertyp aus, d.h. die Gruppe *X1000*, *X1200*, *X4000*.
- Klicken Sie auf **Weiter**.
- Wählen Sie die Softwarekomponenten aus, die Sie installieren wollen. Sie können die voreingestellte Auswahl übernehmen oder selbst eine Auswahl treffen. Sie sollten die Markierung des **Configuration Wizard** nicht aufheben, wenn Sie eine Grundkonfiguration von **X1000** mit dem Configuration Wizard durchführen wollen.
- Klicken Sie auf **Weiter**.
Eine Liste der für die Installation ausgewählten Komponenten erscheint.
- Um diese Komponenten zu installieren, klicken Sie auf **Weiter**.
Die Dateien werden kopiert. Nach kurzer Zeit erscheint ein Meldungsfenster, daß die Installation von BRICKware abgeschlossen ist.
- Wenn Sie eine Neukonfiguration von **X1000** vornehmen möchten, belassen Sie die vorausgewählte Einstellung *Mit der Konfiguration des Geräts fortfahren* und klicken auf **Fertigstellen**.
Der Configuration Wizard startet.

Update Ab BRICKware Version 5.2.1 brauchen Sie eine ältere Version der Software auf Ihrem PC nicht zu deinstallieren, sondern können ein Update durchführen.

- Folgen Sie den Anweisungen auf dem Bildschirm.
Die vorhandenen BRICKware-Dateien auf Ihrem PC werden durch neue ersetzt. Nach kurzer Zeit erscheint ein Meldungsfenster, daß das Update von BRICKware abgeschlossen ist. Klicken Sie auf **Fertigstellen**, um den Update-Vorgang zu beenden.

Aktuelle BRICKware bereits vorhanden Wenn auf Ihrem Rechner bereits eine aktuelle Version der BRICKware gespeichert ist, können Sie während eines erneuten Installationsvorgangs die vorhandene Installation ändern, Sie können einen defekten Teil des Programms wiederherstellen oder BRICKware von Ihrem PC entfernen.

- Folgen Sie den Anweisungen auf dem Bildschirm.
Die Dateien werden kopiert bzw. von Ihrem PC entfernt. Nach kurzer Zeit erscheint ein Meldungsfenster, daß die Wartungsoperationen abgeschlossen sind. Klicken Sie auf **Fertigstellen**, um den Wartungsvorgang zu beenden.

3.4 Lösungsszenarien

In diesem Abschnitt finden Sie einige Konfigurationsbeispiele, die Ihnen bei den häufigsten Konfigurationsanliegen weiterhelfen.



Sie brauchen den Configuration Wizard nur einmal zu durchlaufen, auch wenn Sie mehrere Konfigurationsvorschläge kombinieren möchten.

3.4.1 Zugang zum Internet einrichten

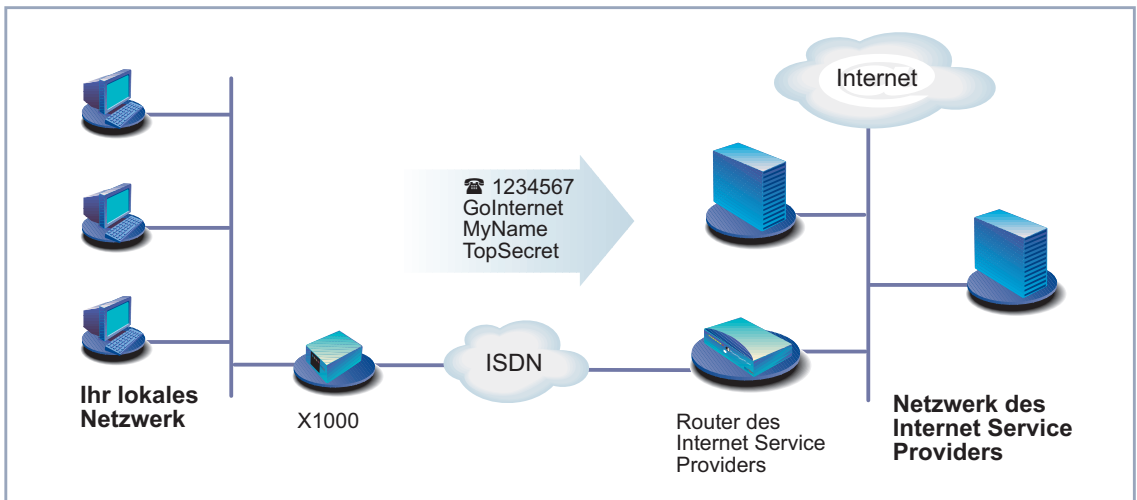


Bild 3-2: **X1000** und Ihr Internet Service Provider

Unter Windows können Sie für **X1000** mit dem Configuration Wizard schnell und einfach einen Zugang zum Internet konfigurieren.

Gehen Sie vor, wie in [Kapitel 3, Seite 35](#) beschrieben. Folgen Sie den Anweisungen auf dem Bildschirm. Beachten Sie dabei:

- Wählen Sie die Konfigurationspunkte (siehe [Kapitel 3.5, Seite 55](#)):

- **Router-Grundkonfiguration**, um die grundlegenden Router-Einstellungen vorzunehmen ([Kapitel 3.5.1, Seite 58](#)).
- **Internet-Anbindung**, um Ihren Internet-Zugang einzurichten ([Kapitel 3.5.2, Seite 62](#)).
- Schließen Sie die Konfiguration ab, wie in [Kapitel 3.5.4, Seite 66](#) beschrieben.
- Wenn Sie von mehreren Rechnern auf das Internet zugreifen möchten, gehen Sie vor wie in [Kapitel 3.7, Seite 71](#) beschrieben.
- Zum Schluß testen Sie Ihre Konfiguration (siehe [Kapitel 3.9, Seite 84](#)).

3.4.2 Kommunikationsanwendungen nutzen

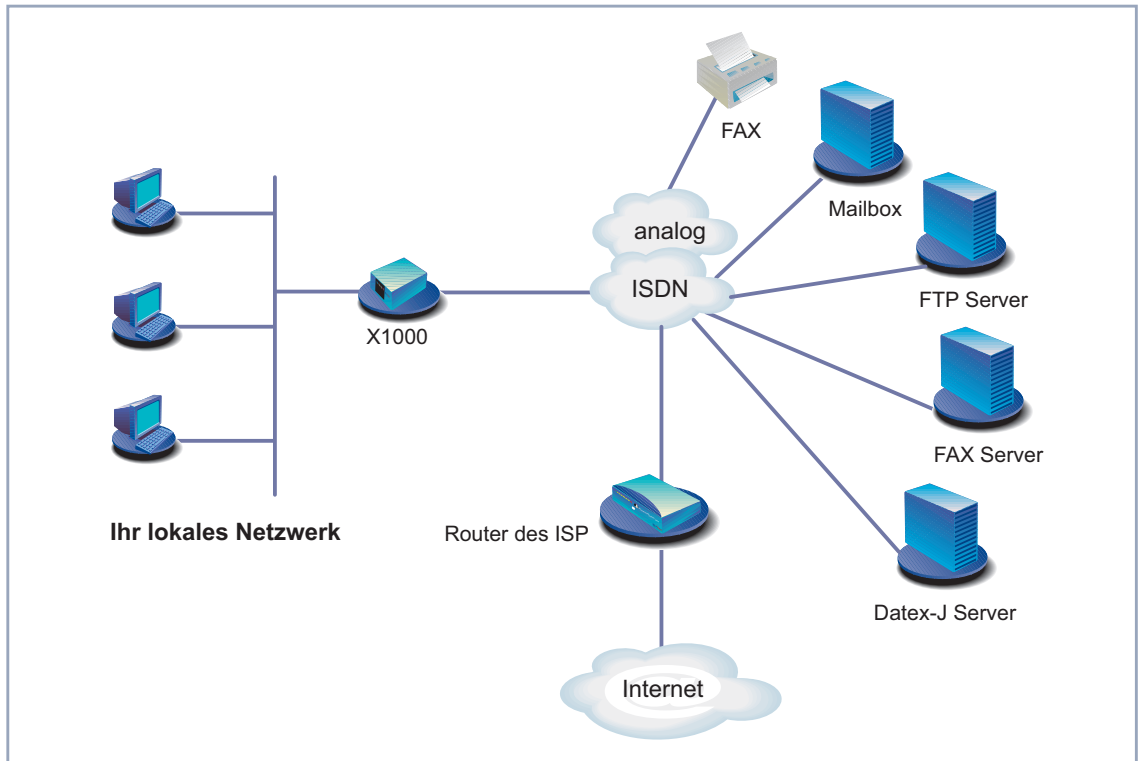


Bild 3-3: **X1000** mit Kommunikationsanwendungen

Verwenden Sie den Configuration Wizard unter Windows, um von mehreren Rechnern aus Kommunikationsanwendungen (z.B. FAX und Anrufbeantworter) zu nutzen.

Gehen Sie vor, wie ab [Kapitel 3.2, Seite 40](#) beschrieben. Folgen Sie den Anweisungen auf dem Bildschirm. Beachten Sie dabei:

- Wählen Sie die Konfigurationen (siehe [Kapitel 3.5, Seite 55](#)):
 - **Router-Grundkonfiguration**, um die grundlegenden Router-Einstellungen vorzunehmen ([Kapitel 3.5.1, Seite 58](#)).

- Schließen Sie die Konfiguration ab wie in [Kapitel 3.5.4, Seite 66](#) beschrieben.
- Konfigurieren Sie die Remote CAPI-Schnittstelle (siehe [Kapitel 3.6, Seite 69](#))
- Richten Sie FAX und Anrufbeantworter ein, wenn gewünscht ([Kapitel 3.8, Seite 77](#)).

3.4.3 Eine Firmenniederlassung an die Firmenzentrale anbinden

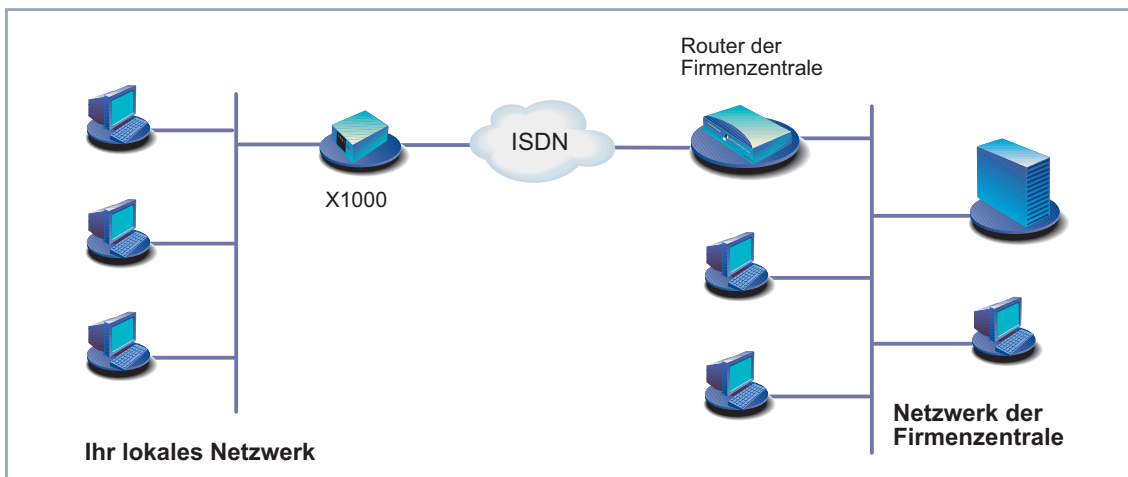


Bild 3-4: X1000 in Ihrer Niederlassung

Mit dem Configuration Wizard unter Windows können Sie Firmenniederlassungen oder Heimarbeitsplätze schnell und einfach an die Firmenzentrale anbinden. Die Mitarbeiter in der Niederlassung oder am Heimarbeitsplatz können dann auf die Daten der Firmenzentrale zugreifen als wären sie vor Ort.

Gehen Sie vor, wie in [Kapitel 3, Seite 35](#) beschrieben. Folgen Sie den Anweisungen auf dem Bildschirm. Beachten Sie dabei:

- Wählen Sie die Konfigurationspunkte (siehe [Kapitel 3.5, Seite 55](#)):

- **Router-Grundkonfiguration**, um die grundlegenden Router-Einstellungen vorzunehmen ([Kapitel 3.5.1, Seite 58](#)).
 - **Firmennetzanbindung**, um eine Firmennetzanbindung z. B. zu einer Firmenzentrale zu ermöglichen ([Kapitel 3.5.3, Seite 64](#)).
- Schließen Sie die Konfiguration ab wie in [Kapitel 3.5.4, Seite 66](#) beschrieben.
- Nehmen Sie zusätzliche Einstellungen an Ihren Rechnern vor ([Kapitel 3.7, Seite 71](#)).

3.4.4 Außendienstmitarbeitern ohne Router Zugang zur Firmenzentrale ermöglichen (Dial-in)

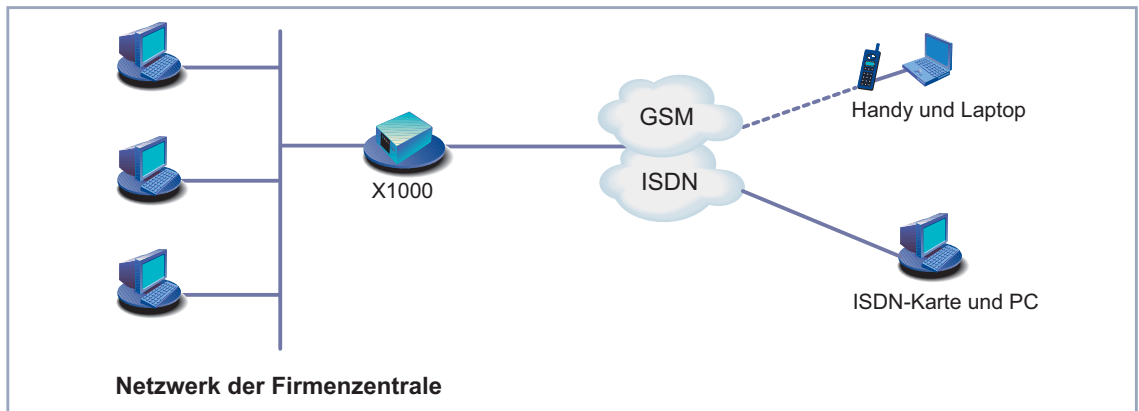


Bild 3-5: **X1000** in der Firmenzentrale

Um einem Außendienstmitarbeiter oder einem Mitarbeiter am Heimarbeitsplatz Zugang zu den Daten seiner Firmenzentrale zu ermöglichen (sogenanntes Dial-in), benötigen Sie für die Konfiguration Ihres **X1000** das Setup Tool.

Ein PC an einem Heimarbeitsplatz kann mittels **DFÜ** über einen ISDN-Anschluß auf das Netz der Firmenzentrale zugreifen.

Der Außendienstmitarbeiter kann sich über Laptop und Handy mit GSM in der Firmenzentrale einwählen.

Zuerst müssen Sie die Grundkonfiguration des Routers durchführen. Sie können dazu den Configuration Wizard (vgl. [Kapitel 3.5.1, Seite 58](#)) oder das Setup Tool (siehe [Kapitel 6, Seite 135](#)) verwenden.

Dann müssen Sie den Mitarbeiter, der auf die Daten der Zentrale zugreifen möchte, als WAN-Partner anlegen. Die genaue Konfiguration erklären wir Ihnen anhand eines Beispiels in [Kapitel 6.2.3, Seite 201](#).

3.5 X1000 unter Windows konfigurieren

Im [Kapitel 3.3, Seite 47](#) haben Sie den Configuration Wizard gestartet, mit dem Sie nun die Konfiguration von **X1000** durchführen. **X1000** muß dafür betriebsbereit sein.

Folgende Konfigurationsschritte stehen zur Wahl:

- Router-Grundkonfiguration
- Internet-Zugang
- Firmennetzanbindung



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

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



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

Die ursprüngliche Konfigurationsdatei von **X1000** können Sie außerdem am Ende der Konfiguration auf dem Router (unter `old_cfg`) sichern, sofern Sie das Paßwort dieser Konfiguration wissen.



Wenn Sie **X1000** direkt an einem Anlagenanschluß (Point-to-Point) betreiben, müssen Sie zusätzlich zu den Einstellungen des Configuration Wizard im Setup Tool eine Eintragung machen. Wählen Sie im Menü **CM-1BRI, ISDN SO** ➤ **INCOMING CALL ANSWERING** für den Ziffernvergleich der eingehenden Nummer den Modus *left to right (DDI)*. Der Wizard nimmt diese Einstellungen nicht automatisch vor, da dies nicht der Standardfall ist. Siehe dazu [Kapitel 6.1.4, Seite 146](#).

Configuration Wizard starten

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



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

Das Startfenster des Configuration Wizard erscheint:



Bild 3-6: Startfenster Configuration Wizard

- Klicken Sie auf **Weiter**.

Konfigurationsmodus einstellen

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

- Wenn Sie wenig Erfahrung mit Netzwerktechnologie haben, wählen Sie den Modus **Quick**. Im folgenden erklären wir die Konfiguration anhand des Quick-Modus.
- Wenn Sie bereits Erfahrung mit Netzwerktechnologie und der Konfiguration von Routern haben, wählen Sie den Modus **Expert**.

So können Sie z. B.:

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



In vielen Fällen reicht die Konfiguration mit dem Quick-Modus aus. Mit dem Expert-Modus können Sie eine Konfiguration von **X1000** optimieren, die Sie mit dem Quick-Modus erstellt haben.

Benutzen Sie jedoch zuerst den Expert-Modus und dann den Quick-Modus, so wird die gesamte Konfiguration überschrieben, die vorherige Konfiguration mit dem Expert-Modus geht verloren.

Serielle Verbindung herstellen

- Klicken Sie auf **Weiter**.

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

- Klicken Sie auf **Weiter**.

Der Configuration Wizard stellt eine Verbindung zu **X1000** her. Der Router wird im Anschluß neu gestartet und der Typ des Routers erkannt: in Ihrem Fall **X1000**.



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

- Prüfen Sie, ob Sie **X1000** richtig angeschlossen haben.
- Prüfen Sie, ob ein Terminal-Programm (z. B. HyperTerminal) oder ein anderes Programm gestartet ist, das die serielle Schnittstelle bereits belegt. Wenn ja, beenden Sie dieses Programm.
- Überlegen Sie, ob Sie die Baudrate bei **X1000** geändert haben. Im Auslieferungszustand sind 9600 Bit/s eingestellt. Wenn Sie die Baudrate verändert haben, stellen Sie wieder 9600 Bit/s ein oder verwenden Sie den Configuration Wizard im Expert-Modus.
- Wenn der Configuration Wizard **X1000** nicht booten konnte, schalten Sie **X1000** aus und wieder ein. Warten Sie, bis die LEDs nicht mehr blinken.
- Klicken Sie auf **Weiter**.

Konfigurationspunkte auswählen

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

- Wählen Sie eine oder mehrere der folgenden Optionen:
 - **Router-Grundkonfiguration**, um die grundlegenden Router-Einstellungen vorzunehmen ([Kapitel 3.5.1, Seite 58](#)).
 - **Internet-Anbindung**, um Ihren Internet-Zugang einzurichten ([Kapitel 3.5.2, Seite 62](#)).

- **Firmennetzanbindung**, um eine Firmennetzanbindung z. B. zu einer Firmenzentrale zu ermöglichen ([Kapitel 3.5.3, Seite 64](#)).

Die grundlegenden Router-Einstellungen müssen Sie in jedem Fall vornehmen.

- Klicken Sie auf **Weiter**.
Eine Zusammenfassung der ausgewählten Konfigurationspunkte wird angezeigt.
- Klicken Sie auf **Weiter**.

3.5.1 Router-Grundkonfiguration einrichten

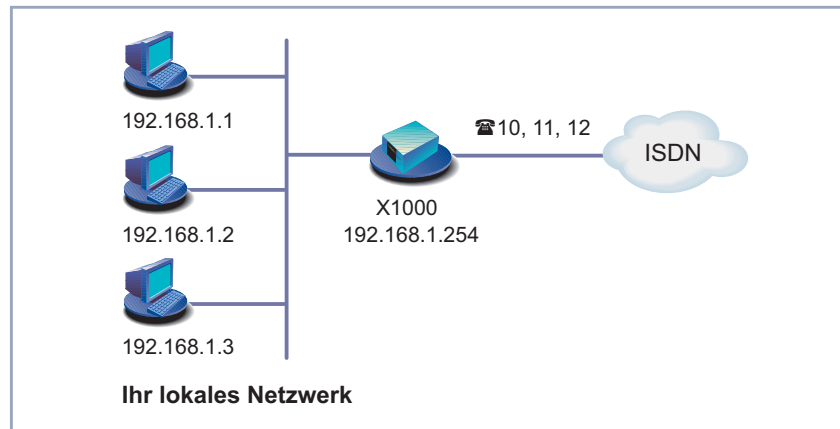


Bild 3-7: Grundkonfiguration von **X1000**



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. Die Vorgehensweise bei der Änderung von Paßwörtern ist unter "[Paßwortänderung](#)", [Seite 128](#) beschrieben.

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

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

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



Je nachdem, wie Ihr PC eingerichtet ist, stellt Ihnen der Configuration Wizard unterschiedliche Konfigurationspunkte zur Verfügung.

Unkonfiguriertes Netzwerk

- Wenn Ihr Rechner noch unkonfiguriert ist, noch keine IP-Adresse hat und als DHCP Client eingerichtet ist, fragt Sie der Configuration Wizard, ob Sie **X1000** als DHCP Server einrichten und die vorgeschlagenen Einstellungen beibehalten wollen.
- Klicken Sie auf **Weiter**.
X1000 erhält die IP-Adresse **192.168.1.254** und vergibt an alle Rechner im Netzwerk automatisch IP-Adressen, beginnend bei **192.168.1.1**.



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

- Deaktivieren Sie das Feld **Diesen Konfigurationsvorschlag übernehmen**.
- Geben Sie als nächstes die IP-Adresse für **X1000** und die zugehörige Netzmaske ein, z. B. **192.168.1.254** und **255.255.255.0**. Klicken Sie auf **Weiter**.
- Geben Sie an, ob Sie **X1000** als DHCP Server einrichten wollen. Wenn ja, geben Sie den IP-Adreßbereich für Ihre PCs ein und bestimmen Sie die Anzahl der IP-Adressen, die von **X1000** vergeben werden.

Denken Sie daran, Ihren Rechnern im Anschluß an die Konfiguration feste IP-Adressen zu geben, falls Sie keinen DHCP Server eingerichtet haben (vgl. [Kapitel 3.7.1, Seite 71](#)).

Bereits konfiguriertes Netzwerk

- Wenn Ihr Rechner eine feste IP-Adresse hat, fragt Sie der Configuration Wizard im Fenster **IP-Adresse des Routers** nach der IP-Adresse von **X1000** im LAN und nach der zugehörigen Netzmaske. Geben Sie die Werte ein, z. B. **192.168.1.254** und **255.255.255.0**.

- Klicken Sie auf **Weiter**.
- Geben Sie ein neues Paßwort für Ihre Zugangsberechtigung ein.
- Klicken Sie auf **Weiter**.
Alle Systempaßwörter sind mit diesem neuen Paßwort versehen.
- Geben Sie die Rufnummern Ihres ISDN-Anschlusses ein, die Sie mit **X1000** verwenden wollen: Geben Sie im Feld **Rufnummern** eine Rufnummer ein und klicken Sie auf **Hinzufügen**. Wiederholen Sie die Eingabe für alle weiteren Rufnummern (vgl. [Bild 3-8](#), [Seite 60](#)).

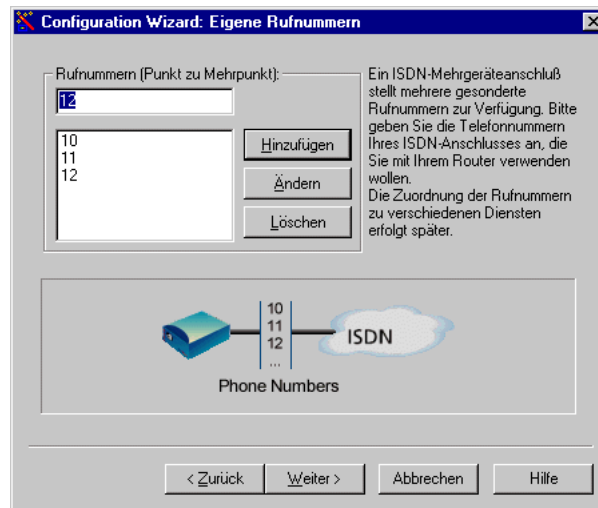


Bild 3-8: Rufnummerneingabe im Configuration Wizard

- Klicken Sie auf **Weiter**.
Der Configuration Wizard ordnet die Rufnummern automatisch bestimmten Diensten zu (mehr zu Diensten und Benutzern in [Kapitel 4.3](#), [Seite 94](#)). Die Zuordnungen können Sie nur im Expert-Modus ändern. (Vgl. [Bild 3-9](#), [Seite 61](#).)

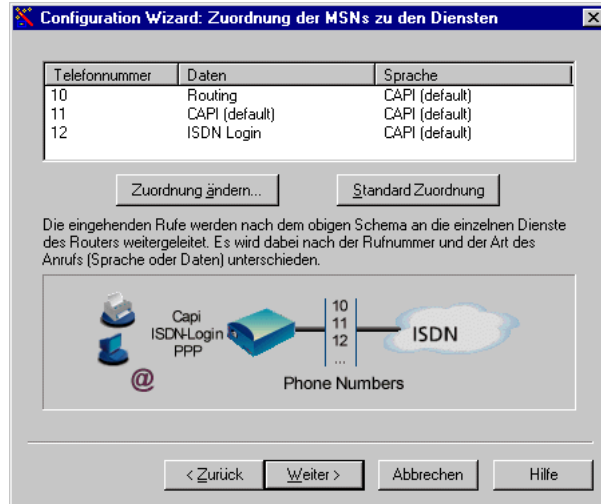


Bild 3-9: Rufnummernzuordnung im Configuration Wizard

➤ Klicken Sie auf **Weiter**.

Die Grundkonfiguration ist beendet. Es erscheint eine Zusammenfassung der Konfigurationsdaten.

Konfiguration im Expert-Modus

Im Expert-Modus können Sie zusätzlich:

- Die Software-Version festlegen, für die Sie die Konfiguration erstellen möchten.
- Die Systemdaten ändern, z. B. Betreuer, Name und Standort von **X1000**.
- Die IP-Adresse eines DNS Servers angeben.
- Ihren Router als DHCP Server einrichten.
- Die Systemzeit von anderer Stelle als vom ISDN beziehen lassen.
- ISDN-Login erlauben.
- Unterschiedliche Systempaßwörter setzen.
- Kommunikationsanwendungen unterschiedlichen Benutzern und Rufnummern zuordnen.

- Unterschiedliche Filter setzen (NetBIOS, CAPI und TAPI Clients).
- Aktivitäten überwachen (Activity Monitor).
- Systemmeldungen protokollieren lassen.
- Die Auslastung von **X1000** überwachen.
- Den Zeitpunkt angeben, wann Gebühreninformationen vom ISDN bezogen werden.
- Nutzerkonten für Telekommunikationsanwendungen (CAPI und/oder TAPI) einrichten.

3.5.2 Mit X1000 ins Internet

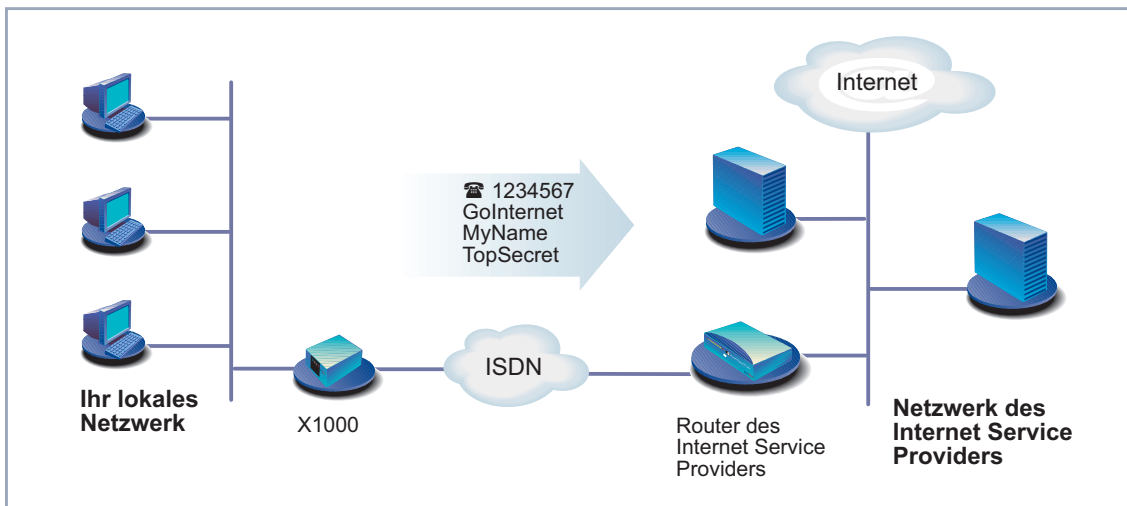


Bild 3-10: **X1000** und Ihr Internet Service Provider

- Klicken Sie auf **Weiter**.
Es erscheint ein Informationsfenster.
- Wenn Sie die Informationen im Fenster gelesen haben, klicken Sie auf **Weiter**.

- Bestimmen Sie als erstes Ihren Internet Service Provider. Wenn Sie Ihren Internet Service Provider in der Liste nicht finden, wählen Sie *anderer Internet Service Provider* aus.

Internet-Testzugang (Internet by call)

Wenn Sie Ihren Internet-Zugang mit **X1000** sofort testen möchten, benötigen Sie keine persönlichen Zugangsdaten eines Internet Service Providers sondern Sie können einen sogenannten "Internet-by-call"-Zugang einrichten.

- Wählen Sie einen Provider aus, der einen Zugang ohne vorherige Anmeldung anbietet. Der Text rechts neben dem angewählten Provider gibt Ihnen darüber Auskunft.
- Klicken Sie auf **Weiter**.
- Geben Sie die Einwahlnummer des Internet Service Providers ein, z. B. **1234567** bzw. übernehmen Sie die voreingestellte Nummer.
- Klicken Sie auf **Weiter**.
- Geben Sie Ihre Teilnehmerkennung (oft Benutzername) und das zugehörige Paßwort ein, z. B. **MyName** und **TopSecret**.
- Klicken Sie auf **Weiter**.

Die Konfiguration Ihres Internetanschlusses ist beendet.

Herkömmlicher Internet-Zugang

Um einen herkömmlichen Internet-Zugang einzurichten, gehen Sie genauso vor wie beim Internet-Testzugang. Sie können in diesem Fall aber eine Verbindung zu jedem beliebigen Internet Service Provider herstellen, von dem Sie vorher Zugangsdaten erhalten haben.

Konfiguration im Expert-Modus

Am Ende jeder Konfiguration erscheint eine Zusammenfassung der Konfigurationsdaten. Im Expert-Modus können Sie zusätzlich:

- IP-Verbindungsdaten protokollieren lassen.
- Komprimierung einschalten.
- Den Verbindungsabbau genauer festlegen (dynamischer und statischer Shorthold).
- Kanalbündelung einschalten. (Dieser Punkt ist nicht für alle Internet Service Provider wählbar).

3.5.3 X1000 ans Firmennetz anbinden

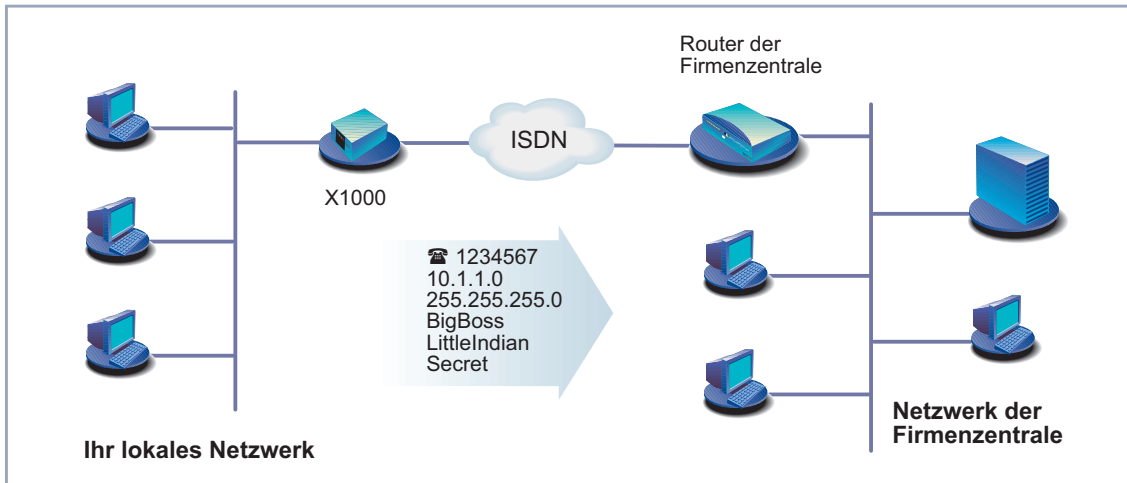


Bild 3-11: **X1000** und Ihre Firmenzentrale

- Klicken Sie auf **Weiter**.
Es erscheint ein Informationsfenster.
- Klicken Sie auf **Weiter**, nachdem Sie die Informationen im Fenster gelesen haben.
Gegebenenfalls erscheint ein weiteres Informationsfenster.
- Klicken Sie auf **Weiter**, nachdem Sie die Informationen im Fenster gelesen haben.
- Geben Sie als erstes den Namen Ihres WAN-Partners (z. B. der Firmenzentrale) und die zugehörige Einwahlnummer ein, z. B. **BigBoss** und **0911987654321**.
Der Name des WAN-Partners muß mit dem Namen übereinstimmen, den Ihr Partner als lokalen Namen verwendet. Ihr Partner muß Anrufe auf die angegebene Einwahlnummer mit dem Dienst Routing annehmen.
- Klicken Sie auf **Weiter**.

- Geben Sie Ihren lokalen Namen und das gemeinsame Paßwort ein, z. B. **LittleIndian** und **Secret**.
Ihr lokaler Name muß mit dem Namen übereinstimmen, den ihr Partner für Sie als WAN-Partner verwendet.
- Klicken Sie auf **Weiter**.
- Fügen Sie eine Route zu Ihrer Firmenzentrale hinzu:
Wenn Sie keinen Internet-Zugang eingerichtet haben, dann wählen Sie **Default Route verwenden**.
Wenn Sie einen Internet-Zugang eingerichtet haben, dann geben Sie selbst die Route ein: Klicken Sie auf **Hinzufügen**. Geben Sie die IP-Adresse oder Netzadresse und die Netzmaske ein, z. B. **10.1.1.0** und **255.255.255.0**. Anhand der Route legen Sie die Verbindung zu Ihrem WAN-Partner (z. B. Firmenzentrale) fest (vgl. [Bild 3-12](#), [Seite 65](#)).



Bild 3-12: Route zum WAN-Partner im Configuration Wizard festlegen



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

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

- Klicken Sie auf **OK**.
- Wenn Ihre Zentrale ein Netzwerk aus mehreren Einzelnetzen betreibt, und Sie in jedes dieser Einzelnetze gelangen wollen, dann geben Sie für jedes weitere Einzelnetz eine Route ein (vgl. [Bild 4-3](#), [Seite 105](#)).
- Klicken Sie auf **Weiter**.

Die Konfiguration Ihres WAN-Partners ist beendet. Es erscheint eine Zusammenfassung der Konfigurationsdaten.

Konfiguration im Expert-Modus

Im Expert-Modus können Sie zusätzlich:

- Eine automatische Rückruffunktion einrichten, damit nur einer der beiden Partner die Telefongebühren übernimmt.
- Die Rufnummer des Anrufers prüfen: Calling Line Identification (CLID).
- IP-Verbindungsdaten protokollieren lassen.
- Überprüfen der Rückroute (Back Route Verify) aktivieren, um die Einspeisung von manipulierten Datenpaketen zu verhindern.
- Komprimierung, Verschlüsselung und Kanalbündelung definieren.
- Den Verbindungsabbau genauer festlegen (dynamischer und statischer Shorthold).

3.5.4 Konfiguration abschließen

- Klicken Sie auf **Weiter**.
- Wählen Sie **Bestehende Konfiguration auf dem Router sichern**, um eine bereits vorhandene Konfiguration von **X1000** vor Überschreiben zu sichern.

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

Der Configuration Wizard loggt sich auf **X1000** ein. Eine bestehende Konfiguration wird als old_cfg auf dem Router gesichert. Die neu erstellte Konfiguration wird zu **X1000** übertragen und zusätzlich auf Ihrem Rechner unter dem Namen brick.cf im Installationsverzeichnis BRICK gespeichert. Nach einiger Zeit erscheint eine Meldung, daß die Konfiguration abgeschlossen ist.



Falls eine Fehlermeldung erscheint, daß der Configuration Wizard sich nicht auf dem Router einloggen konnte, weil das Paßwort geändert ist, gehen Sie folgendermaßen vor:

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

Der Configuration Wizard versucht, sich auf **X1000** einzuloggen.

- Wenn Sie das Paßwort nicht wissen, klicken Sie auf **nicht bekannt** und anschließend auf **OK**.

X1000 wird in den Auslieferungszustand zurückversetzt, sämtliche vorherigen Konfigurationen gehen verloren.



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

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

- Klicken Sie auf **OK**.

Wenn Sie **X1000** als DHCP Server und Ihre Rechner als DHCP Clients eingerichtet haben (Standardfall), dann weist **X1000** den PCs jetzt die IP-Adressen zu. Unter Windows NT bzw. Windows 2000 (Programm IPCONFIG) geschieht dies automatisch, unter Windows 95 (Programm WINIPCFG) müssen Sie die Zuweisung bestätigen.

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

Es erscheint eine Meldung, ob Sie den CAPI Client konfigurieren wollen.

- Klicken Sie auf **Ja**.

Das Fenster Remote Clients Configuration erscheint:

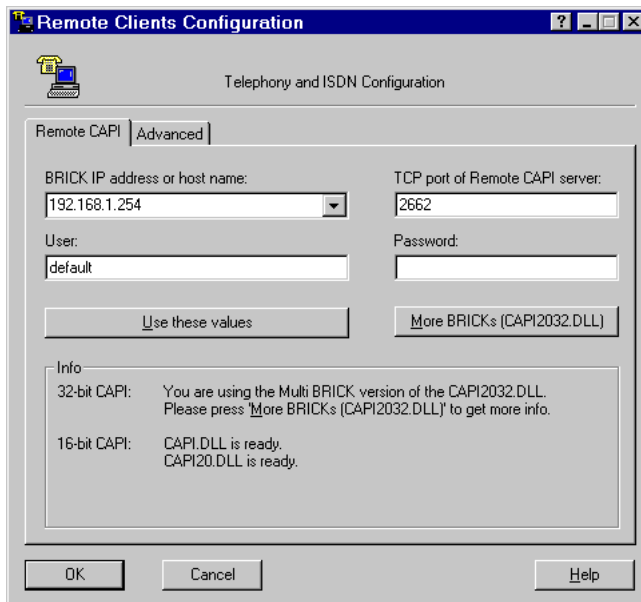


Bild 3-13: Remote-CAPI-Konfiguration

3.6 Remote-CAPI-Schnittstelle am PC

Im ►► **Remote-CAPI-Konfigurationsprogramm** tragen Sie **X1000** als CAPI-Server ein.

Der CAPI-Server von **X1000** ermöglicht:

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

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

Auf dem ersten PC haben Sie bereits BRICKware installiert und das Konfigurationsfenster für die Remote-CAPI-Konfiguration erhalten (vgl. [Bild 3-13, Seite 68](#)). Sie können gleich mit [Kapitel 3.6.2, Seite 70](#) fortfahren. Für alle weiteren PCs im Netz müssen Sie zunächst das Programm CAPI Configuration installieren und die Remote-CAPI-Schnittstelle konfigurieren, wie in [Kapitel 3.6.1, Seite 69](#) und [Kapitel 3.6.2, Seite 70](#) beschrieben.

3.6.1 Remote CAPI Client auf allen weiteren PCs installieren

- Wenn noch nicht geschehen, installieren Sie BRICKware wie im [Kapitel 3.3, Seite 47](#) beschrieben. Wenn von einem PC aus keine Administrationsaufgaben ausgeführt werden sollen, schalten Sie die **Werkzeuge zur Administration** aus.
- Folgen Sie den Anweisungen auf dem Bildschirm.
- Klicken Sie auf **OK**.

Das Remote-CAPI-Konfigurationsfenster erscheint (vgl. [Bild 3-13, Seite 68](#)).

3.6.2 Remote CAPI konfigurieren

Gehen Sie folgendermaßen vor (siehe [Bild 3-13, Seite 68](#)):

- Geben Sie im Register **Remote CAPI** die IP-Adresse von **X1000** ein, z. B. **192.168.1.254**.
- Wenn Sie den Quick-Modus im Configuration Wizard verwendet haben, behalten Sie im Feld **User** den Eintrag **default** bei.
- Wenn Sie im Expert-Modus des Configuration Wizard mehrere Benutzer eingerichtet haben, dann geben Sie den Benutzernamen und ein Paßwort ein. Die Rechte, die Sie während der Konfiguration für diesen Benutzer festgelegt haben, sind damit am aktuellen PC gültig.
- Klicken Sie auf **Use these values**.
Nach kurzer Zeit erscheint eine Meldung "Remote CAPI is ready".
- Wenn keine Fehlermeldung erscheint, klicken Sie auf **OK**.



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

- die IP-Adresse von **X1000** stimmt.
- Sie die Lizenzdaten richtig eingetragen haben.
- Sie einen gültigen Benutzer und das richtige Paßwort eingegeben haben.
- die richtige Port-Nummer 2662 eingetragen ist.
- Ihr Rechner als DHCP Client konfiguriert ist und vielleicht noch keine IP-Adresse bekommen hat (siehe [Kapitel 4.4, Seite 98](#)).

- Wiederholen Sie die Remote-CAPI-Installation auf allen PCs im Netz, auf denen Sie Kommunikationsanwendungen (z. B. Fax) ermöglichen wollen.



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

3.7 PC einrichten

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

■ Wenn Sie mit dem Configuration Wizard **X1000** nicht als DHCP Server eingerichtet und die Rechner bisher keine IP-Adressen haben, müssen Sie (gemäß [Kapitel 3.7.1, Seite 71](#)):

- die IP-Adressen jetzt festlegen
- den Rechnern den "Weg nach draußen" (Gateway, DNS Server) zeigen

Falls Sie die Standardeinstellungen des Configuration Wizard übernommen haben und Sie Ihre PCs als DHCP Clients eingerichtet haben, brauchen Sie das [Kapitel 3.7.1, Seite 71](#) nicht berücksichtigen. **X1000** liefert in diesem Fall die nötigen Informationen automatisch.

■ Wenn Sie eine Firmennetzanbindung konfiguriert haben, wollen Sie sicherlich Rechner aus dem Partner-LAN (z. B. Firmenzentrale) über Ihr Windows erreichen. Dazu müssen Sie vorgehen, wie in [Kapitel 3.7.2, Seite 73](#) beschrieben.

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

Falls Sie **X1000** nicht als DHCP Server eingerichtet und Ihre Rechner noch keine IP-Adressen haben, müssen Sie den Rechnern jetzt sagen, unter welcher IP-Adresse sie erreichbar sein sollen. Zusätzlich müssen Sie den Rechnern mitteilen, wo der "Weg nach draußen", z. B. ins Internet führt. Gehen Sie folgendermaßen vor:

- Windows 95/98**
- Klicken Sie im Windows-Startmenü auf **Einstellungen** ➤ **Systemsteuerung**.
 - Doppelklicken Sie auf **Netzwerk**.
 - Klicken Sie auf **TCP/IP** ➤ **Eigenschaften**.

- Geben Sie im Register **IP-Adresse** eine eindeutige IP-Adresse für Ihren Rechner und die Netzmaske ein, z. B. **192.168.1.1** und **255.255.255.0**.
 - Geben Sie im Register **Gateway** die IP-Adresse von **X1000** ein, z. B. **192.168.1.254**. Klicken Sie auf **Hinzufügen**.
 - Wenn Sie keinen eigenen DNS Server haben, geben Sie im Register **DNS Konfiguration** unter **Suchreihenfolge für DNS Server** die IP-Adresse von **X1000** ein, z. B. **192.168.1.254**.
- Windows NT**
- Klicken Sie im Windows-Startmenü auf **Einstellungen** ▶ **Systemsteuerung**.
 - Doppelklicken Sie auf **Netzwerk**.
 - Wählen Sie das Register **Protokolle**. Klicken Sie auf **TCP/IP-Protokoll** ▶ **Eigenschaften**.
 - Klicken Sie im Register **IP-Adresse** auf **IP-Adresse angeben** und bestimmen Sie IP-Adresse, Netzmaske und Standard-Gateway, z. B. **192.168.1.254**, **255.255.255.0** und **192.168.1.1**. Als Standard-Gateway tragen Sie die IP-Adresse von **X1000** ein.
 - Klicken Sie im Register **DNS** unter **Suchreihenfolge des DNS-Dienstes** auf **Hinzufügen** und geben Sie die IP-Adresse von **X1000** ein, z. B. **192.168.1.254**.
- Windows 2000**
- Klicken Sie im Windows-Startmenü auf **Einstellungen** ▶ **Netzwerk- und DFÜ-Verbindungen**.
 - Doppelklicken Sie auf **LAN-Verbindung**.
 - Klicken Sie im Register **Allgemein** auf **Eigenschaften**.
 - Wählen Sie im Register **Allgemein** das **Internetprotokoll (TCP/IP)**. Klicken Sie auf **Eigenschaften**.
 - Aktivieren Sie im Register **Allgemein** den Punkt **Folgende IP-Adresse verwenden**. Bestimmen Sie IP-Adresse, Netzmaske und Standard-Gateway, z. B. **192.168.1.254**, **255.255.255.0** und **192.168.1.1**. Als Standard-Gateway tragen Sie die IP-Adresse von **X1000** ein.
 - Wenn Sie keinen eigenen DNS Server haben, geben Sie als DNS-Server-Adresse die IP-Adresse von **X1000** ein. Aktivieren Sie den Punkt **Folgende DNS-Serveradressen verwenden**.
 - Geben Sie die Adresse ein, z. B. **192.168.1.254** und klicken Sie auf **OK**.

- Schließen Sie die offenen Fenster mit **OK** bzw. **Schließen**.
- Zum Schluß**
- Bestätigen Sie alle Eingaben und starten Sie zum Schluß den Rechner neu.
 - Wiederholen Sie die Installation für alle Rechner im Netz.

3.7.2 Die Rechner des Partnernetzes finden

Sie haben jetzt bei **X1000** alles für eine Verbindung zu Ihrem Partnernetz eingestellt. Nun wollen Sie beispielsweise von Ihrem PC aus auf den Windows-Rechner **BossPC** im Partnernetz zugreifen.



Dabei ist einiges zu beachten. Jeder Rechner in Ihrem LAN oder im Netzwerk Ihres Partners benötigt eine eindeutige Adresse, die IP-Adresse. In der Vergangenheit haben sich außer IP-Adressen auch sogenannte Computer- und Host-Namen entwickelt, um Rechner über deren Namen (wie z. B. **BossPC**) anzusprechen. Die Computer-Namen werden speziell in Windows-Netzwerken verwendet. Rechner verstehen aber nur IP-Adressen und keine Namen. Daher muß es eine Stelle geben, welche die zu den Namen gehörigen IP-Adressen bekannt gibt, d.h. eine Namensauflösung durchführt (vgl. [Kapitel 4.5, Seite 101](#)). Typische Beispiele für eine solche Namensauflösung sind ein DNS- oder ein WINS Server. Da Sie in einem kleinen Netzwerk meist keinen eigenen Server einrichten, gibt es eine andere Möglichkeit, wie Sie den Namen **BossPC** in eine IP-Adresse auflösen können: die LMHOSTS-Datei.

In der LMHOSTS-Datei ordnen Sie tabellarisch IP-Adressen den verschiedenen Computer-Namen zu. Wenn Sie dann nach dem Rechner **BossPC** suchen, der sich im Partnernetz (z. B. Firmenzentrale) befindet, fragt Ihr Rechner seine LMHOSTS-Datei nach der zugehörigen IP-Adresse und kann so den Rechner finden. Alternativ können Sie DNS Proxy (siehe [Kapitel 7.3.2, Seite 273](#)) verwenden.



Achtung!

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

- Um ungewollte Gebühren zu vermeiden, sollten Sie **X1000** unbedingt überwachen. Benutzen Sie dazu das Taschengeldkonto (siehe [Kapitel 8.1.3, Seite 317](#)).



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

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

Außerdem sollten Sie beachten,

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



Sie können sich auch komplett an der Windows-NT-Domäne eines Partnernetzes anmelden. Um eine solche Konfiguration zu testen, stellt BinTec für Sie einen Testzugang bereit. Wie Sie diesen Zugang einrichten, erfahren Sie unter www.bintec.de.

Sie können Ihrem PC die IP-Adresse des Rechners **BossPC** mitteilen, indem Sie die LMHOSTS-Textdatei bearbeiten. Da Sie die erforderlichen Eintragungen aber für jeden Rechner in Ihrem LAN vornehmen müssen, ist diese Metho-

de zwar möglich aber umständlich und arbeitsaufwendig. Wir empfehlen Ihnen stattdessen, DNS Proxy (siehe [Kapitel 7.3.2, Seite 273](#)) zu verwenden.

Um die LMHOSTS-Textdatei zu bearbeiten:

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

Nach kurzer Zeit erscheint der Rechnername.

Verknüpfung auf dem Desktop

- Damit Sie den Rechner **BossPC** nicht bei jedem Neustart Ihres Rechners erneut suchen müssen, rechtsklicken Sie auf das Rechnersymbol und klicken Sie auf **Verknüpfung herstellen**.
Es erscheint die Frage, ob Sie eine Verknüpfung auf dem Desktop erstellen wollen.
- Klicken Sie auf **Ja**.
Sie können jetzt jederzeit über Windows auf den Rechner **BossPC** des Partnernetzes zugreifen.

Netzlaufwerk verbinden

Eine andere Möglichkeit eine Netzlaufwerksverbindung herzustellen ist:

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

3

Los geht's

➤ Klicken Sie auf **OK**.

3.8 Fax und Anrufbeantworter einrichten mit RVS-COM Lite

Faxen machen. Aber wie?

Nachdem Sie Rechner und **X1000** erfolgreich konfiguriert haben, installieren Sie RVS-COM Lite. Mit RVS-COM Lite können Sie:

- Faxe verschicken und empfangen
- Einen Anrufbeantworter einrichten
- Dateitransferdienste und Eurofile-Transferdienste einrichten

In den nachfolgenden Abschnitten beschreiben wir, wie Sie Ihrem Rechner und **X1000** das Faxen mit RVS-COM Lite (Version 1.63) beibringen und eine Anrufbeantworterfunktion einrichten.



Mit **X1000** haben Sie genau eine Einzelplatzlizenz für RVS-COM Lite erhalten. Falls Sie RVS-COM Lite auf mehreren Rechnern installieren wollen, wenden Sie sich bitte an RVS Datentechnik GmbH. Die Anschrift können Sie der Online-Hilfe von RVS-COM Lite entnehmen.

3.8.1 RVS-COM Lite installieren

- Legen Sie Ihre BinTec Companion CD erneut in das CD-ROM-Laufwerk Ihres PCs ein.
Nach kurzer Zeit erscheint automatisch das Startfenster.
- Wenn das Startfenster nicht automatisch erscheint, klicken Sie im Windows Explorer auf Ihr CD-ROM-Laufwerk und doppelklicken Sie auf **set-up.exe**.
- Klicken Sie im Startfenster auf **RVS-COM Lite**.
Das Setup-Programm startet.
- Geben Sie Ihre RVS-COM-Lizenznummer ein. Die Nummer befindet sich auf Ihrer Lizenzkarte.
- Klicken Sie auf **Installieren**.
Das Startfenster erscheint.

- Bestätigen Sie die beiden folgenden Fenster und geben Sie das Verzeichnis an, in das RVS-COM Lite installiert werden soll. Klicken Sie auf **Weiter**. Die Dateien werden kopiert. Nach kurzer Zeit erscheint ein Hinweis, daß das Setup-Programm beendet ist.
 - Klicken Sie auf **Beenden**.
- Das Startfenster des Installationsassistenten erscheint:

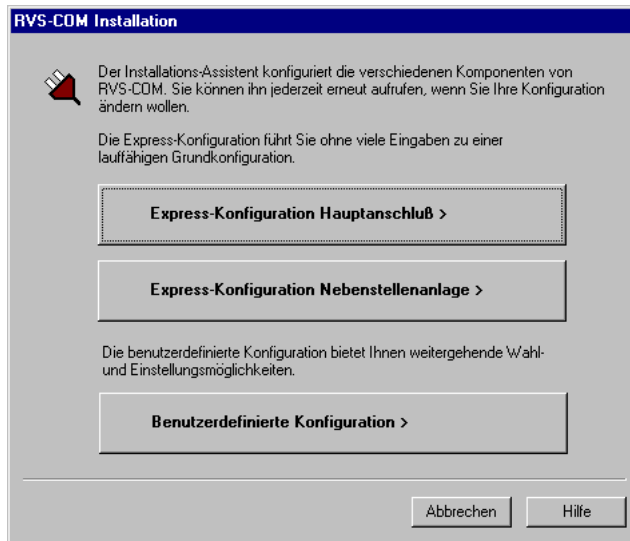


Bild 3-14: Startfenster des Installationsassistenten von RVS-COM Lite



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

- Prüfen Sie, ob Sie **X1000** mit Ihrem ISDN-Anschluß verbunden haben.
- Prüfen Sie, ob Ihre Remote-CAPI-Konfiguration eingerichtet ist, wie in Kapitel [Kapitel 3.6.2, Seite 70](#) beschrieben.



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

- Wenn **X1000** an einem Hauptanschluß (z. B. NTBA-Adapter) angeschlossen ist, klicken Sie auf **Express-Konfiguration Hauptanschluß**.
- Wenn **X1000** an einer TK-Anlage angeschlossen ist, klicken Sie auf **Express-Konfiguration Nebenstellenanlage**.
- Klicken Sie auf **Weiter**.
Es erscheint ein Hinweis, daß Sie RVS-COM für den Betrieb mit einem ISDN-Adapter mit CAPI-Schnittstelle konfiguriert haben.
- Klicken Sie auf **Weiter**.
- Wenn ein Hinweis erscheint, daß Sie Wahlparameter (z. B. Amts- oder Ortskennzahl) ändern sollten, bestätigen Sie die Meldung, um Ihre Wahlparameter richtig einzustellen. Passen Sie die Einstellungen an (vgl. [Bild 3-15](#), Seite 79).



Bild 3-15: Wahlparameter



Die Ortskennzahl muß ohne führende "0" angegeben sein.

Die Amtskennzahlen brauchen Sie nur, wenn Sie **X1000** an einer TK-Anlage betreiben. Meist stimmen hier die Amtskennzahlen für Orts- und Ferngespräche überein (siehe [Bild 3-15, Seite 79](#)).

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



Wenn Sie **X1000** direkt an einem Anlagenanschluß (Point-to-Point) betreiben, müssen Sie zusätzlich zu den Einstellungen des Configuration Wizard im Setup Tool eine Eintragung machen. Wählen Sie im Menü **CM-1BRI, ISDN SO** ➤ **INCOMING CALL ANSWERING** für den Ziffernvergleich der eingehenden Nummer den Modus *left to right (DDI)*. Der Configuration Wizard nimmt diese Einstellungen nicht automatisch vor, da dies nicht der Standardfall ist. Siehe dazu [Kapitel 6.1.4, Seite 146](#).

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

Die Konfiguration mit dem Installationsassistenten ist abgeschlossen.

3.8.2 RVS-COM Lite einrichten

Im folgenden müssen die Nummern, die Sie auch mit dem Configuration Wizard für den CAPI-Dienst festgelegt haben, den verschiedenen Kommunikationsanwendungen (Fax, Anrufbeantworter) zugewiesen werden. Das nachfolgende

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

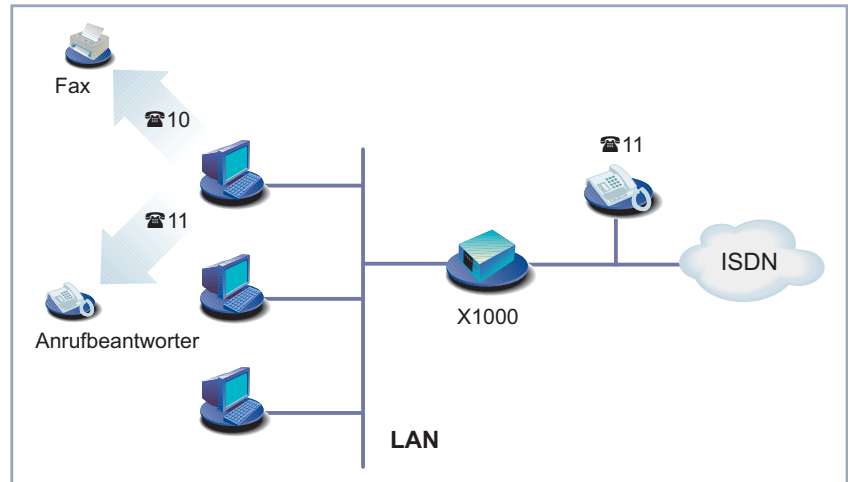


Bild 3-16: Szenario: 1 Telefon, 1 Rechner mit Fax und Anrufbeantworter



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

- Klicken Sie im Windows-Startmenü auf **Programme** ➤ **RVS-COM Lite** ➤ **CommCenter**.
- Klicken Sie im Register **Rufnummern** auf **Hinzufügen**, um weitere Rufnummern einzugeben. Geben Sie die Nummern ein, die Sie bereits bei der Router-Konfiguration mit dem Configuration Wizard verwendet haben (vgl. [Bild 3-17, Seite 82](#)).

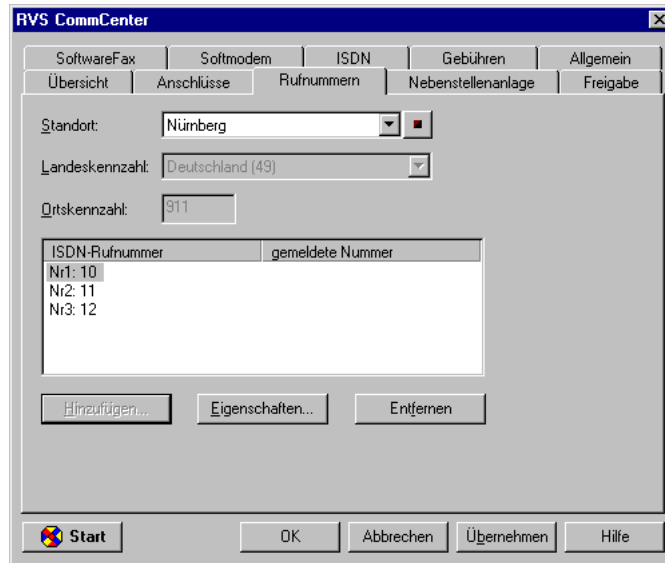


Bild 3-17: Rufnummernkonfiguration in RVS-COM Lite

- Wenn Sie alle Rufnummern eingegeben haben, klicken Sie auf **Übernehmen**. Vergewissern Sie sich, daß im Register **SoftwareFax** die Punkte **SoftwareFax soll zum Fax-Versand verwendet werden** und **SoftwareFax soll zum Fax-Empfang verwendet werden** aktiv sind.
- Klicken Sie im Register **Anschlüsse** auf **Eigenschaften**, um die Rufnummern den unterschiedlichen Diensten zuzuweisen (vgl. [Bild 3-18](#), [Seite 83](#)).



Bild 3-18: Zuordnung der Rufnummern zu Diensten in RVS-COM Lite

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

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

3.9 Konfiguration testen

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

3.9.1 Internet-Zugang testen

- Konfigurieren Sie Ihren Browser, falls Sie dies noch nicht getan haben. Wenn Sie von Ihrem Internet Service Provider die IP-Adresse eines Proxy Servers erhalten haben, können Sie die IP-Adresse des Proxy Servers eintragen. Achten Sie darauf, daß Sie eine Verbindung über Ihr lokales Netzwerk einrichten.
- Geben Sie in Ihrem Browser www.bintec.de ein.
Die Homepage von BinTec Communications AG erscheint.

3.9.2 E-Mails verschicken und empfangen

- Legen Sie im E-Mail-Programm einen "Account" an, falls Sie noch keinen haben. Die Server für Incoming und Outgoing Mail haben Sie von Ihrem Internet Service Provider erhalten. Achten Sie darauf, daß Sie eine Verbindung über Ihr lokales Netzwerk einrichten.
- Schicken Sie eine E-Mail an einen guten Bekannten oder – wenn Sie wollen – direkt an BinTec! Verwenden Sie dazu die E-Mail-Adresse testmail@bintec.de und geben Sie als Betreff Testmail ein.
Sie erhalten von uns umgehend eine Rückantwort, damit Sie kontrollieren können, ob alles geklappt hat.

3.9.3 Ein Fax verschicken

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

Zunächst stellen Sie sicher, daß bei jedem Fax mehrere Sendeveruche unternommen werden, falls das Fax nicht auf Anhieb verschickt werden kann.

- Klicken Sie im Windows-Startmenü auf **Programme** ➤ **RVS-COM Lite** ➤ **CommCenter**.
- Klicken Sie auf **Start** und dann auf **Inbox**.
Sie erhalten eine Liste der empfangenen und versandten Faxe.
- Klicken Sie auf **Fax** ➤ **EinstellungenFax**.
Im Register **Zeitplan** stellen Sie ein, wieviele Sendeveruche Sie bei einem Fax unternehmen möchten und wieviel Zeit zwischen den einzelnen Versuchen verstreichen soll.
- Geben Sie die Anzahl der Versuche ein, z. B. **3**.
- Geben Sie die Wartezeit zwischen den Versuchen ein, z. B. **5** Minuten.
- Klicken Sie auf **OK**.
- Schließen Sie **Inbox** und **RVSCommCenter**.

Erstellen Sie das gewünschte Fax und versenden Sie es anschließend.

- Klicken Sie im Windows-Startmenü auf **Programme** ➤ **RVS-COM Lite** ➤ **Neues Fax erstellen**.
Das Fenster **RVS Fax: Empfänger** erscheint.
- Geben Sie Rufnummer, z. B. **967310**, und Name des Empfängers ein.
- Klicken Sie auf **Weiter**.
- Geben Sie einen Betreff ein und wählen Sie das Deckblatt **Normal** aus.
- Klicken Sie auf **Weiter**.
- Geben Sie einen kurzen Text ein, z. B. **Testfax**.
- Klicken Sie auf **Weiter**.
- Wenn Sie wollen, können Sie jetzt noch eine Datei anhängen, die Sie mit Ihrem Fax zusammen verschicken.

- Klicken Sie auf **Weiter** und anschließend auf **Senden**.

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

Wenn Sie an sich selbst ein Fax geschickt haben, sollten Sie das Fax umgehend erhalten (vgl. [Kapitel 3.9.4, Seite 86](#)). So können Sie am besten kontrollieren, ob Ihre Fax-Anwendung funktioniert.



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

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

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

3.9.4 Ein Fax empfangen



Da es sich bei der Fax-Lösung mit **X1000** und RVS-COM Lite um eine Softfax-Lösung handelt, muß die Fax-Software immer gestartet sein, wenn Sie Faxe empfangen wollen. Bei der Installation von RVS-COM Lite wird in der Task-Leiste von Windows automatisch RVS-COM Lite abgelegt – solange Sie RVS-COM Lite nicht beenden, ist die Applikation jederzeit empfangsbereit.

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

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

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



Bild 3-19: RVS Inbox

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

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

4 Grundlagen



Damit Sie einige Zusammenhänge und die Funktionsweise von **X1000** besser verstehen, erklären wir in diesem Kapitel einige Grundlagen von **X1000** und Netzwerktechnik im Allgemeinen.

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

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



Falls Sie alles noch genauer wissen wollen, als wir es hier beschreiben, dann sollten Sie in unserer Software Reference nachschlagen. Dort finden Sie alle technischen Zusammenhänge im Detail beschrieben.

4.1 ISDN-Grundlagen

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

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

Um Daten über ISDN zu übertragen, wird u.a. das Protokoll **PPP** (Point-to-Point Protocol) verwendet.

Jeder ISDN-Basisanschluß (S₀-Anschluß) besteht aus drei Kanälen:

- 2 B-Kanäle
- 1 D-Kanal

B-Kanal Kanalbündelung Die B-Kanäle dienen der Datenübertragung (Sprache, Text, Daten). Jeder B-Kanal hat eine Datenübertragungsrate von 64 kBit/s. Da Sie zwei B-Kanäle haben, können Sie, wie Sie sicherlich wissen, von zwei Telefonen aus gleichzeitig mit verschiedenen Teilnehmern telefonieren. Auch **X1000** kann beide B-Kanäle gleichzeitig nutzen, um Daten mit zwei verschiedenen Gegenstellen auszutauschen. Sie können sogar beide B-Kanäle "zusammenfassen", um Daten zu einer einzigen Gegenstelle über beide Kanäle zu übertragen. Sie zahlen dann zwar für beide B-Kanäle Telefongebühren, brauchen aber zur Übertragung der Daten nur die halbe Zeit. Dies können Sie bei **X1000** über die Funktion Kanalbündelung erreichen. Kanalbündelung können Sie im Expert-Modus des Configuration Wizard oder mit dem Setup Tool (vgl. [Kapitel 7.2.2, Seite 224](#)) konfigurieren.

D-Kanal Der D-Kanal dient dem Verbindungsaufbau und übermittelt Steuerinformationen mit einer Datenübertragungsrate von 16 kBit/s. Solche Steuerinformationen dienen z. B. der Identifizierung des Anrufers (Calling Party's Number = Nummer des Anrufers) und des Angerufenen (Called Party's Number = Nummer des Angerufenen) über deren Rufnummern. Sie können Ihren Router z. B. so konfigurieren, daß er nur Gespräche von Partnern entgegennimmt, bei de-

nen die über den D-Kanal gemeldete Rufnummer mit der Rufnummer übereinstimmt, die Sie für den Partner definiert haben. Man nennt diesen Sicherheitsmechanismus Calling Line Identification – kurz CLID. Andere Authentisierungsmechanismen überprüfen Benutzername und Paßwort der Gegenstelle.

CLID können Sie nur im Expert-Modus des Configuration Wizard oder im Setup Tool einstellen.

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

Gebühreninformation und Shorthold

Bei vielen ISDN-Anschlüssen erhalten Sie Gebühreninformationen. Meistens erhalten Sie diese Informationen am Ende einer Verbindung, bei einigen ISDN-Anschlüssen sogar während einer Verbindung (AOCD: advice of charge during the call; diese Funktion müssen Sie oft gesondert beantragen). **X1000** kann diese Informationen auswerten, damit Sie Kosten sparen.

Normalerweise (im Quick-Modus) ist **X1000** so konfiguriert, daß er nach einer bestimmten Zeit (standardmäßig 20 Sekunden) die Verbindung beendet, wenn keine Daten mehr fließen. Nach diesem festen Zeitraum, in dem keine Daten mehr ausgetauscht werden, baut **X1000** die Verbindung ab – auch wenn gerade ein neues Gebührenintervall angebrochen ist (statischer Shorthold).

Wenn Sie nun sicher wissen, daß Sie während einer Verbindung Gebühreninformationen bekommen, können Sie diesen Verbindungsabbau weiter optimieren und gerade angebrochene Einheiten noch ausnützen. Wenn **X1000** regelmäßig Gebühreninformationen durch das ISDN erhält, können Sie Ihrem Router sagen, daß er eine Verbindung erst kurz vor Beginn der nächsten Gebühreninformationen abbauen soll (dynamischer Shorthold). Die Angabe der Zeitspanne erfolgt hier nicht in Sekunden, sondern in Form eines Prozentwertes, der sich an einem Gebührenintervall orientiert (z. B. soll die Verbindung abgebaut werden, wenn 80% eines Gebührenintervalls verbraucht ist). Den dynamischen Shorthold können Sie nur im Expert-Modus des Configuration Wizard oder im Setup Tool einstellen (vgl. [Kapitel 6.2.1, Seite 169](#)).

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

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

MSN

Im Quick-Modus des Configuration Wizard haben Sie Ihre Rufnummern eingetragen. Wir hatten angegeben, daß es genügt, nur jeweils die Stellen anzugeben, in denen sich die Rufnummern unterscheiden (meist die letzten beiden Stellen). **X1000** beginnt die Überprüfung der Rufnummern normalerweise von hinten (Modus right to left). Sobald die in der Konfiguration eingetragene Nummer der eingehenden Nummer entspricht, kann der Ruf einem Dienst eindeutig zugeordnet werden. Sie müssen daher nicht jedesmal die kompletten MSNs eintragen.

Bei einer Nebenstellenanlage haben Sie normalerweise eine Basisrufnummer und mehrere Durchwahlnummern. Hier sollten Sie sich auf jeden Fall über Besonderheiten Ihres Anschlusses erkundigen. Es kann nämlich sein, daß Rufnummern intern (S₀-Bus) bei verschiedenen Nebenstellenanlagen unterschiedlich gemeldet werden. Da Sie aber immer die gemeldeten Rufnummern angeben müssen, auf die **X1000** (oder auch RVS-COM Lite) reagieren soll, sollten Sie diese gemeldeten Rufnummern wissen. Falls Sie nicht wissen, wie Ihre Nebenstellenanlage die Rufnummern weiterreicht, können Sie das auch über **X1000** herausfinden (siehe [Kapitel 6.1.4, Seite 146](#)).

4.2 Wenn es noch schneller gehen soll...

Mit Kompressionsverfahren erreichen Sie in der gleichen Zeit einen höheren Datendurchsatz. Bei Kompressionsverfahren müssen Sie aber immer sicherstellen, daß Ihre Gegenstelle das entsprechende Kompressionsverfahren unterstützt. Sonst kommt keine Verbindung zustande. Im Quick-Modus des Configuration Wizard haben Sie keine Komprimierung aktiviert. Dazu müssen Sie den Expert-Modus oder das Setup Tool verwenden (vgl. [Kapitel 7.2.9, Seite 259](#)).

X1000 unterstützt:

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

Bei ADSL-Anschlüssen anderer Internet Service Provider liegen unter Umständen vom T-DSL-Anschluß der Deutschen Telekom AG abweichende Gegebenheiten vor. Auskünfte über Ihren Anschluß erhalten Sie von Ihrem Provider.

4.3 Dienste und Benutzer

Abwicklung eines Anrufs Jeder Router benutzt intern einen Algorithmus, um auf eingehende Rufe aus dem ISDN zu reagieren. **X1000** kann die eingehenden Rufe auf folgende Dienste verteilen:

- PPP (Routing)
- ISDN-Login
- CAPI

Was also macht so ein Dienst? Der Dienst PPP ist der allgemeine Routing-Dienst von **X1000**. Damit wird eingehenden Datenrufen von WAN-Partnern eine Wählverbindung mit Ihrem LAN ermöglicht. So können Sie es Partnern außerhalb Ihres lokalen Netzwerkes ermöglichen, auf Rechner in Ihrem LAN zuzugreifen.

Der Dienst ISDN-Login ermöglicht eingehenden Daten- und Sprachrufen Zugang zur SNMP-Shell von **X1000**. So kann **X1000** z. B. aus der Ferne konfiguriert und gewartet werden.

Der Dienst CAPI ermöglicht eingehenden Daten- und Sprach-Rufen eine Verbindung mit Kommunikationsanwendungen auf Hosts im LAN, die auf die Remote-CAPI-Schnittstelle von **X1000** zugreifen. So können beispielsweise mit **X1000** verbundene Hosts Faxe empfangen.

CAPI und Remote CAPI Die meisten Kommunikationsprogramme verwenden die genormte CAPI-Schnittstelle. Mit ihr sind die typischen Dienste wie Anrufbeantworter, Fax (herkömmliches und digitales Fax), Dateitransfer und Eurofile-Transfer über ISDN möglich. Die CAPI-Schnittstelle allein ermöglicht nur jeweils einem Rechner, die Dienste über den ISDN-Anschluß zu nutzen. Mit Unterstützung der BinTec-eigenen Remote CAPI ist es allen Teilnehmern im Netz möglich, diese Dienste zu nutzen, sofern jeder Teilnehmer die entsprechende Anwender-Software installiert hat. Alle Teilnehmer teilen sich einen einzigen ISDN-Anschluß.

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

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

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

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

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

In unserem Konfigurationsbeispiel (vgl. [Bild 3-16, Seite 81](#)) haben wir die Nummer **10** als Faxnummer verwendet und die Nummer **11** für einen Anrufbeantworter. Wie Sie sicherlich bemerkt haben, ist die Nummer **10** zweimal vergeben: für PPP und CAPI.

Sprache oder Daten?

Da bei der Rufannahme außer der Rufnummer auch zwischen Daten- und Sprachrufen unterschieden wird, ist diese Doppelbelegung für **X1000** kein Problem. **X1000** erkennt bei einem eingehenden Fax auf der Nummer **10**, daß es sich um Sprachdaten (Töne) handelt und leitet die Informationen an den CAPI-Dienst weiter. Wenn sich hingegen ein WAN-Partner in Ihr Netz einwählt, handelt es sich um digitale Informationen (Daten) und **X1000** leitet die Daten an den Dienst PPP.

Daten sind:

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

Sprache sind:

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

Wer ist schneller? Wir sind außerdem davon ausgegangen, daß Sie unter der Nummer **11** auch über ein Telefon erreichbar sind, das am gleichen S₀-Bus angeschlossen ist wie **X1000**. Alle Geräte, die am gleichen S₀-Bus angeschlossen sind und die unter der gleichen Rufnummer erreichbar sind, reagieren auch auf Anrufe. D. h. bei einem eingehenden Ruf unter der Nummer **11** klingelt Ihr Telefon, gleichzeitig fühlt sich aber auch RVS-COM Lite angesprochen. Da Sie bei RVS-COM Lite die Anzahl der Klingelzeichen vor der Rufannahme angegeben haben, wartet RVS-COM Lite erst einmal ab. Falls Sie den Hörer zuerst abnehmen, sind Sie schneller und erhalten den Ruf. Falls Sie nicht rechtzeitig am Apparat sind, bevor die Anzahl der Klingelzeichen von RVS-COM Lite erreicht ist, ist RVS-COM Lite schneller und nimmt den Ruf entgegen.

Mehrere Benutzer Eine Rufnummer haben wir nicht besetzt: die **12**. Falls Sie ein Netzwerk mit zwei Rechnern im LAN haben, könnten Sie theoretisch jedem dieser zwei Rechner eine eigene Faxnummer zuweisen. Im RVS CommCenter von Rechner 1 würden Sie weiterhin die **11** als Rufnummer eingetragen lassen, im RVS CommCenter von Rechner 2 würden Sie die Nummer **12** als Rufnummer für Fax eintragen (vgl. [Bild 4-1, Seite 96](#)).

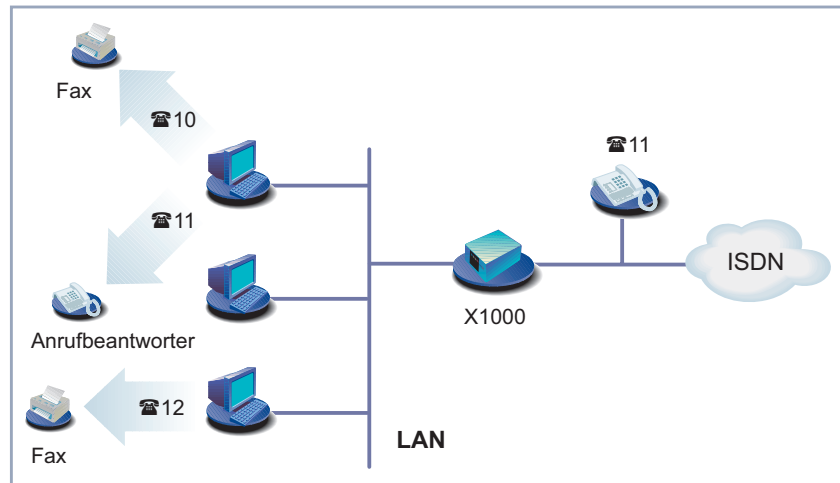


Bild 4-1: Szenario: 2 Rechner, 2 Faxnummern, 1 Telefon

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

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

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

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

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

Mehrere Nutzerkonten Jeder Anwender, dem bestimmte Kommunikationsanwendungen gestattet werden sollen, erhält einen eigenen Benutzernamen und ein eigenes Paßwort. Die Einstellungen für Name und Paßwort müssen Sie auf dem Router (z. B. über den Configuration Wizard im Expert-Modus oder im Setup Tool [Kapitel 7.1.2, Seite 216](#)) und auf dem jeweiligen Rechner vornehmen (Remote-CAPI-Konfiguration). Zusätzlich bestimmen Sie auf dem Router für jeden Anwender eine eigene Rufnummer (z. B. Faxnummer). Auf die Rufnummer reagiert nur die Kommunikationsanwendung des Rechners, bei dem auch in der CAPI-Konfiguration der zugehörige Nutzer eingetragen ist.

4.4 X1000 als DHCP Server

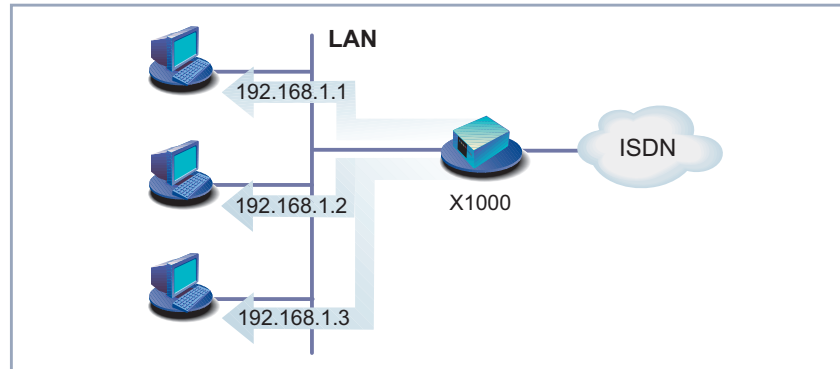


Bild 4-2: **X1000** als DHCP Server

Wozu IP-Adressen? Jeder Rechner in Ihrem LAN benötigt, wie auch **X1000**, eine eigene Adresse. Sonst können die Geräte untereinander nicht kommunizieren. Wenn Sie einen Brief mit der Post verschicken, müssen Sie auch Absender und Adressat angeben – andernfalls kommt der Brief weder an, noch kann er an Sie zurückgeschickt werden.

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

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

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



X1000 kann nicht als DHCP Client eingerichtet werden. Es ist aber möglich, **X1000** über einen BootP Server eine IP-Adresse zuzuweisen (vgl. [Kapitel 5.1.2, Seite 115](#)).

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

X1000 als DHCP Server

Sie können **X1000** als DHCP Server verwenden, wenn Sie keinen anderen DHCP Server haben (vgl. [Kapitel 6.1.5, Seite 159](#)). Er vergibt an alle Geräte des eigenen Netzes IP-Adressen. Eventuell haben Sie im Quick-Modus mit dem Configuration Wizard **X1000** bereits als DHCP Server eingerichtet. Wenn Sie die vorgeschlagenen Werte übernommen haben, dann erhalten jetzt Ihre Rechner IP-Adressen von **192.168.1.1** bis **192.168.1.8**.

Wann werden IP-Adressen zugeteilt?

Jeder Rechner, der sich neu am Netz anmeldet – weil er z. B. neu gestartet wurde – sendet eine Adreßanforderung (Request) aus und erhält daraufhin seine IP-Adresse. Diese Adresse erhält der Rechner meist nur für einen definierten Zeitraum (im Setup Tool können Sie diesen Zeitraum einstellen). Danach wird die Adresse neu zugewiesen. Sie können Ihrem Rechner aber auch explizit sagen, daß er jetzt eine IP-Adresse bekommen soll. Dies hat der Configuration Wizard im Quick-Modus für Sie getan, falls Sie **X1000** als DHCP Server eingerichtet haben.

Unter Windows 95 bzw. Windows 98 rufen Sie das Programm WINIPCFG auf, um IP-Adressen zu überprüfen oder neu zuzuweisen. Unter Windows NT bzw. Windows 2000 verwenden Sie das Programm IPCONFIG.

Windows 95/98 WINIPCFG aufrufen

- Klicken Sie im Windows-Startmenü auf **Ausführen**.
- Geben Sie `winipcfg` ein.
Es erscheint ein Fenster, in dem Sie die IP-Adresse Ihres Rechner und andere Netzinformationen sehen.
- Um eine IP-Adresse neu zuzuweisen, klicken Sie auf **Renew**.

Windows NT IPCONFIG aufrufen

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

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

Windows 2000 IPCONFIG aufrufen

- Klicken Sie im Windows-Startmenü auf **Programme** ➤ **Zubehör** ➤ **Eingabeaufforderung**.
- Geben Sie `ipconfig` oder `ipconfig/all` ein, um die IP-Adresse Ihres Rechners und andere Netzinformationen abzufragen.
- Geben Sie `ipconfig/renew` ein, um eine IP-Adresse neu zuzuweisen.
- Geben Sie `ipconfig/release` ein, um eine IP-Adresse freizugeben.

4.5 Wie funktioniert Namensauflösung?

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

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

- DNS Server (im LAN, beim Internet Service Provider oder im Partnernetz)
- **X1000** als DNS Proxy:
 - Auf dem PC ist die IP-Adresse von **X1000** als DNS Server eingetragen.
 - **X1000** ist als DHCP Server, Ihre Rechner sind als DHCP Clients konfiguriert und bekommen automatisch die IP-Adresse von **X1000** mitgeteilt, die dann für DNS-Anfragen verwendet wird.
- WINS Server
- HOSTS- und LMHOSTS-Datei

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

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

X1000 als DNS Proxy Wenn Sie **X1000** als DNS Proxy verwenden (Standardfall), leitet Ihr Router alle DNS-Anfragen an ihm bekannte DNS Server weiter (im Normalfall ein DNS Server beim Internet Service Provider).

WINS Speziell in Windows-Netzwerken gibt es den Dienst WINS. Über WINS können Sie nur Computer-Namen oder sogenannte NetBIOS-Namen auflösen, aber keine Host-Namen. Analog zu TCP/IP wird NetBIOS als Transportprotokoll ver-

wendet. Meist sind in Windows-Netzwerken Computer- und Host-Namen identisch.

HOSTS- und LMHOSTS-Datei

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

Wie funktioniert Namensauflösung in der Praxis?

Internetzugang

Wenn Sie mit dem Configuration Wizard einen Internetzugang einrichten und keinen eigenen DNS Server haben, bezieht **X1000** normalerweise die IP-Adresse eines Domain Name Servers vom Internet Service Provider automatisch. Auf den PCs im LAN ist **X1000** als DNS Proxy bekannt. Bei einer Anfrage zur Namensauflösung (z. B. für www.bintec.de) fragt der PC beim Router, der Router wiederum beim DNS Server des Internet Service Providers nach. So kann die Adresse aufgelöst werden.

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

Internetzugang und Firmennetzanbindung

Wenn Sie zusätzlich zur Internet-Anbindung eine Firmennetzanbindung einrichten, Sie **X1000** als DNS Proxy verwenden und die DNS-Einstellungen von **X1000** zum Internet Service Provider führen (Standardfall), würden alle Anfragen zur Namensauflösung an Ihren Provider gestellt. Wenn Sie nun einen Rechner im Partnernetz (**BossPC**) erreichen wollen, würde **X1000** eine Verbindung zum Provider aufbauen und dort nach der IP-Adresse von **BossPC** fragen. Computer-Namen allerdings sind im Gegensatz zu Adressen wie www.bintec.de nicht im Internet bekannt. Sie werden nur innerhalb eines Firmennetzes verwendet (Domäne, Arbeitsgruppe). Der Domain Name Server beim Provider könnte deshalb den Namen normalerweise nicht auflösen. Der Verbindungsaufbau wäre unnötig, Sie können **BossPC** trotzdem nicht erreichen.

Damit solche ungewollten und nutzlosen Verbindungen nicht zustande kommen, müssen Sie verhindern, daß solche Anfragen nach Rechnernamen im Partnernetzes gestellt werden. Diese Aufgabe übernimmt der einfache NetBIOS-Filter für Sie (siehe [Kapitel 4.7, Seite 107](#)).

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

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

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

Wie Sie in der LMHOSTS-Datei einen Eintrag erstellen, haben wir bereits in [Kapitel 3.7.2, Seite 73](#) erklärt.

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

- Domänen- und Arbeitsgruppennamen müssen in Ihrem und im Partnernetz gleich sein.
- Sie müssen beim Partnernetz als Benutzer bekannt sein.
- Sie dürfen mit dem Configuration Wizard keine umfangreiche NetBIOS-Filterung eingestellt haben (siehe [Kapitel 4.7, Seite 107](#)), sonst können bestimmte Windows-Funktionen wie z. B. eine Netzlaufwerksverbindung nicht genutzt werden.



Das Thema "Verbindung von Windows-Netzwerken" ist sehr komplex und umfangreich. Eine Reihe von Faktoren bestimmen den Erfolg eines solchen Vorhabens. Da eine genauere Behandlung dieses Themas den Rahmen unseres Handbuches sprengen würde, können wir an dieser Stelle nur auf andere Fachliteratur verweisen, z. B. "Windows NT 4.0 Connectivity Guide" von Richard Grace (ISBN 0-7645.3160-3) oder die Microsoft Knowledge Base im World Wide Web unter www.support.microsoft.com/directory.

4.6 Was sind Routen und Default-Routen?

Routen Um IP-Pakete zu einem Partnernetz oder einem Internet Service Provider verschicken zu können, muß **X1000** wissen, welche Pakete wohin geleitet werden sollen.

Dafür definieren Sie Wege bzw. Routen. Die Routen führen zu einem bestimmten Netzwerk mit einer definierten
 >> **Netzadresse** und einer
 >> **Netzmaske**. Für jedes

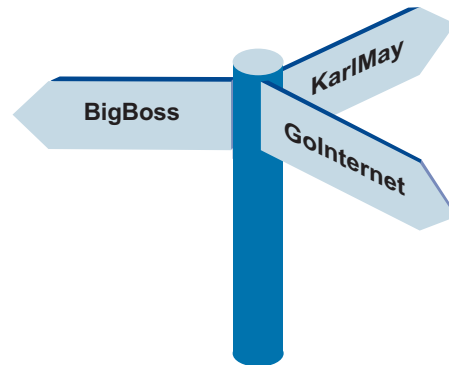
Netz, in das Sie gelangen wollen, geben Sie eine solche Route an. Sie bestimmen beispielsweise die Route zu Ihrem WAN-Partner (Firmenzentrale). Alle Pakete, deren IP-Adressen zur Netzmaske und Netzadresse dieser Route passen, werden dann an dieses Partnernetz geschickt.

Wohin aber mit allen übrigen IP-Paketen?

Default-Route Anhand einer sogenannten Default-Route können Sie bestimmen, daß alle Pakete, deren Ziel **X1000** unbekannt ist, zu einem bestimmten Netz geschickt werden (Default-Route). Üblicherweise verwendet man für die Default-Route die Route zum Internet Service Provider, da die meisten unbekanntesten Pakete als Ziel das Internet haben (z. B. www.bintec.de). Der Configuration Wizard hat die Route zu Ihrem Provider automatisch als Default-Route eingetragen, sofern Sie einen Internet-Zugang eingerichtet haben. Wenn Sie nur ein Partnernetz, nicht aber einen Internet-Zugang einrichten, verwendet der Configuration Wizard einfach als Default-Route die Route zu Ihrem Partnernetz.



Wenn Sie keinen Internet-Zugang haben, hingegen Ihre Firmenzentrale einen Internet Service Provider hat, können Sie über die Firmenzentrale ins Internet. Indem Sie die Default-Route zu Ihrer Zentrale eingerichtet haben, dort alle unbekanntesten Pakete ankommen, und Ihr Partnernetz wiederum alle unbekanntesten IP-Pakete zu einem Internet Service Provider routet, können Sie in Absprache mit Ihrem WAN-Partner über das Partnernetz ins Internet.



Mehrere Routen für einen WAN-Partner

Das Netzwerk der Firmenzentrale kann aus mehreren LANs mit unterschiedlichen Netzadressen und Netzmasken bestehen (Subnetze). In diesem Fall müssen Sie für jedes Subnetz, das Sie in der Firmenzentrale erreichen wollen, eine eigene Route angeben (vgl. [Bild 4-3, Seite 105](#)).

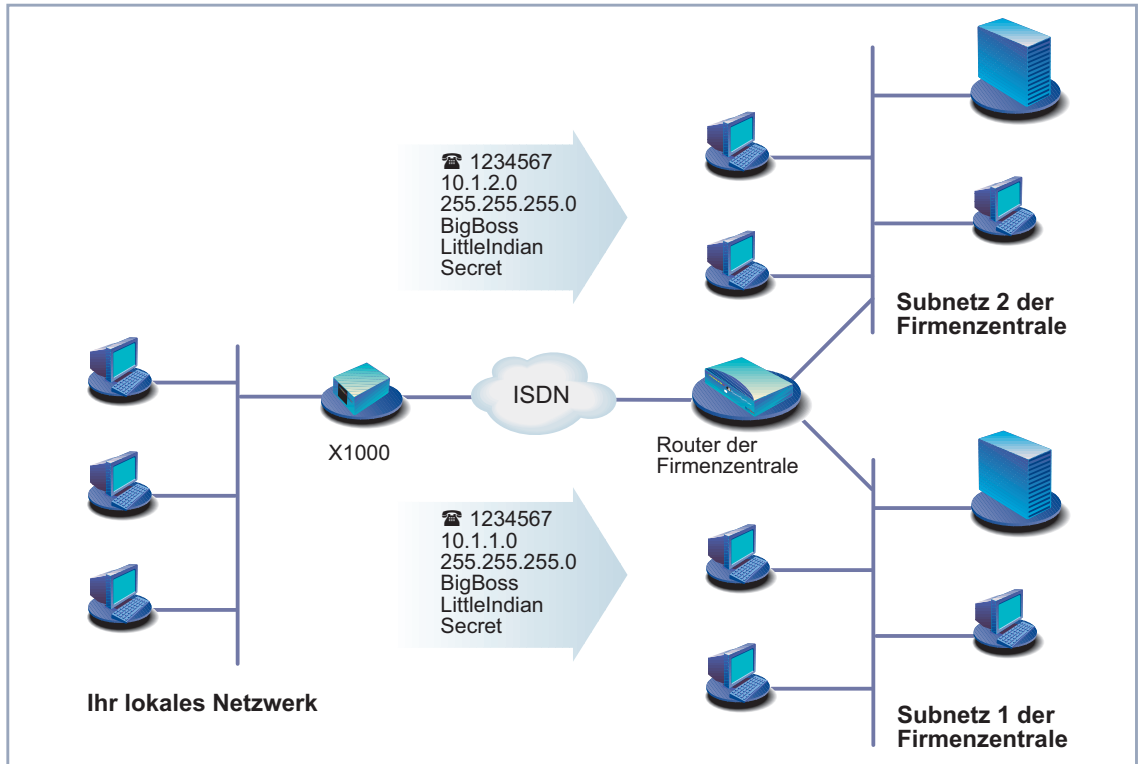


Bild 4-3: Szenario: WAN-Partner mit zwei Subnetzen

Routen, Namensauflösung und Gateway

Nicht nur **X1000** sondern auch Ihre Rechner kennen so etwas wie eine Default-Route: das Gateway. Alle Pakete, deren Ziel nicht innerhalb des eigenen Netzes liegt, schickt Ihr Rechner zu diesem Gateway. Als Gateway dient **X1000**. Sobald Ihr Router ein solches Paket empfängt, schickt er es wiederum über eine seiner Routen (z. B. zum Internet Service Provider oder einem anderen Partnernetz) weiter.

Angenommen **X1000**'s Default-Route führt zum Internet Service Provider, Ihre Rechner sind DHCP Clients und bekommen ihre IP-Adresse von **X1000** zuge-

wiesen. In diesem Fall bekommen die Rechner auch die IP-Adresse von **X1000** als DNS Proxy und Gateway mitgeteilt. (Das Beispiel funktioniert auch, wenn Ihre PCs keine DHCP Clients sind, aber so konfiguriert sind, daß die IP-Adresse von **X1000** als DNS Server und Gateway eingetragen ist.)

Sobald Sie z. B. **www.bintec.de** im Browser eingeben, schickt der PC eine DNS-Anfrage an **X1000** – **X1000** ist ja als DNS Proxy bekannt. **X1000** selbst schickt als DNS Proxy das Paket mit der DNS-Anfrage zum Internet Service Provider. Dort kann der Name **www.bintec.de** aufgelöst werden, die DNS-Anfrage ist erfolgreich und der Rechner erhält als Antwort die IP-Adresse zum Namen **www.bintec.de** zurück. Nun kann das Paket auf die eigentliche Reise zu **www.bintec.de** geschickt werden. Da **X1000** als Gateway eingetragen ist, und das Paket eine IP-Adresse hat, die nicht innerhalb des eigenen Netzes liegt, wird das Paket über das Gateway **X1000** nach außen geschickt. Da für die IP-Adresse zu **www.bintec.de** keine eigene Route eingetragen ist, verwendet **X1000** die Default-Route.

4.7 Filter und NetBIOS

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

Warum Filter? Jedes Windows-Netzwerk verwendet Computer-Namen. Heißt Ihr Rechner z. B. Winnetou, ein anderer Rechner im Netz OldShatterhand, dann sind diese Computer-Namen im Internet nicht bekannt, da sie nur innerhalb eines Firmennetzes verwendet werden (anders als bei Adressen wie www.bintec.de). Diese Computer-Namen werden in jedem Windows-Netzwerk über den Dienst NetBIOS aufgelöst. NetBIOS wiederum versucht, diese Computer-Namen über Ihren Internet Service Provider aufzulösen. **X1000** würde ständig (die Abfragen sind ca. alle 12 bis 15 min und somit recht häufig!) eine unnötige Verbindung mit Ihrem Provider herstellen, da der Provider die WINS-Namen nicht auflösen kann. Die Namen sind ja nur in Ihrem Netz (Arbeitsgruppe, Domäne) bekannt.

Hier kommen die Filter ins Spiel.

Einfache NetBIOS Filter Wenn Sie mit dem Configuration Wizard den einfachen NetBIOS-Filter aktiviert haben, werden alle IP-Pakete verworfen, die zu **X1000** für eine NetBIOS-Namensauflösung geschickt werden. Der Configuration Wizard konfiguriert im Quick-Modus für LAN-LAN-Kopplung immer eine einfache Filterung.

Umfangreiche NetBIOS Filter Eine umfangreiche Filterung nimmt der Configuration Wizard im Quick-Modus automatisch vor, wenn zwar Internetzugang aber keine Firmennetzanbindung konfiguriert wird. Im Expert-Modus oder mit dem Setup Tool können Sie zwischen keiner, einfacher und umfangreicher Filterung wählen. Beim umfangreichen Filter wird der ganze NetBIOS-Datenverkehr (NetBIOS-Broadcasts) gefiltert – also nicht nur die Anfragen zur Namensauflösung. Auswirkungen: Alle Dienste von NetBIOS wie das gemeinsame Nutzen von Laufwerken und Druckern können nicht verwendet werden.

CAPI-Filter Zusätzlich können Sie im Expert-Modus mit dem Configuration Wizard auch noch einen CAPI-Filter einrichten. Nehmen wir an, Sie haben in Ihrer CAPI-Konfiguration statt der IP-Adresse von **X1000** aus Versehen eine falsche IP-Adresse eingegeben. Ihre Rechner würden CAPI-Anfragen immer an die falsche Adresse schicken. Da die falsche IP-Adresse sich vielleicht außerhalb Ihres Netzes befindet, versucht **X1000**, das entsprechende IP-Paket an Ihren Internet Service Provider zu leiten. Also wieder ein unnötiger Verbindungsauf-

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



Mit Filtermechanismen können Sie nicht nur ungewollte Verbindungen vermeiden. Die primäre Funktion von Filtern ist Sicherheit des eigenen Netzes vor Zugriffen von außen (vgl. [Kapitel 8.2.8, Seite 338](#)).

4.8 MIB und SNMP

Was ist SNMP? SNMP (Simple Network Management Protocol) ist ein Protokoll, das zur Protokollfamilie TCP/IP gehört. Mit Hilfe von SNMP werden Managementinformationen von Netzwerkkomponenten (z. B. Router, Drucker, Rechner) in einem Netz transportiert. Es wird verwendet, um die Geräte in einem Netzwerk zu überwachen und zu verwalten. Die Überwachung erfolgt dabei von zentraler Stelle aus über einen SNMP-Manager. Dieser SNMP-Manager ist ein Programm, das über SNMP Daten von den Geräten im Netz anfordern kann. Ein Administrator, der diesen SNMP-Manager bedient, kann alle Geräte in seinem Netz von einem Standort aus überwachen. SNMP definiert als Protokoll die Regeln, mit denen sich dann das Managementprogramm mit den Clients (z. B. **X1000**) unterhält. Auf Ihrer BinTec Companion CD befindet sich ein solcher SNMP-Manager, der Configuration Manager (für Windows-Betriebssysteme). Statt des Configuration Managers können Sie zur Verwaltung Ihres Netzes aber auch jeden anderen beliebigen SNMP-Manager verwenden, z. B. HP OpenView. Statt eines graphisch orientierten Programmes können Sie sogar auch direkt auf Kommandozeilenebene arbeiten (SNMP-Shell).

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

In einer MIB sind Objekte gespeichert (Information Base), die über SNMP abgefragt, geändert oder erzeugt werden können (Management). Die Objekte selbst sind Informationscontainer, in die Informationen abgelegt werden, um Zustände und Werte des Objekts zu definieren. Ein Objekt, das Sie selbst bei der Konfiguration Ihres Routers mit dem Configuration Wizard geändert haben, ist z. B. das Objekt, in dem Ihre Zugangsberechtigung zu **X1000** abgelegt ist. Ursprünglich war der Wert *bintec* als Paßwort definiert, jetzt ist dort Ihr eigener Wert abgelegt.

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

5 Ein Draht zu X1000

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

Sie erfahren,

- wie Sie auf **X1000** zugreifen.
- wie Sie sich einloggen.
- welche Konfigurationsmöglichkeiten Ihnen zur Verfügung stehen.
- wie das **Setup Tool** aufgebaut ist.

5.1 Zugangsmöglichkeiten

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

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

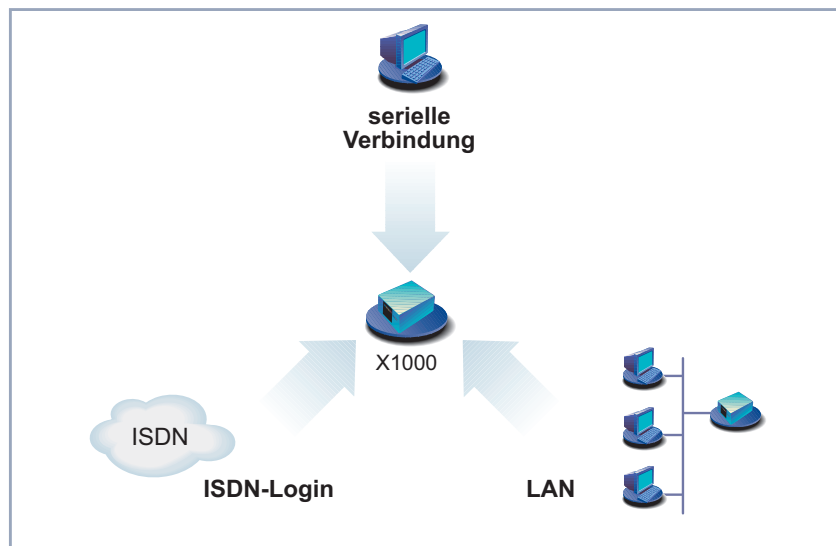


Bild 5-1: Zugangsmöglichkeiten zu **X1000**

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

Mit dem **Configuration Manager** (BRICKware for Windows) unter Windows greifen Sie über das LAN auf **X1000** zu. Mit dem Configuration Wizard greifen Sie über die serielle Schnittstelle auf **X1000** zu.

5.1.1 Zugang über die serielle Schnittstelle

Erstkonfiguration Der Zugang über die serielle Schnittstelle ist gut geeignet, wenn Sie eine Initialkonfiguration von **X1000** durchführen. Um **X1000** über die serielle Schnittstelle an Ihren Rechner anzuschließen, gehen Sie vor wie in [Kapitel 3.1, Seite 37](#) erläutert.

Windows Wenn Sie einen Windows-PC benutzen, benötigen Sie für die serielle Verbindung ein Terminal-Programm, z. B. **HyperTerminal**.



Stellen Sie sicher, daß **HyperTerminal** bei der Windows-Installation auf dem PC mitinstalliert wurde.

Beachten Sie, daß bei Windows 98 und Windows ME **HyperTerminal** nicht in der Standardinstallation enthalten ist.

Wenn Sie **HyperTerminal** unter Windows 2000 oder Windows ME benutzen, kann es sein, daß die Cursor-Tasten zur Navigation im Setup Tool nicht funktionieren. Benutzen Sie in diesem Fall die Tabulator-Taste oder **Strg+P** zum Bewegen in Vorwärtsrichtung und **Strg+N** für die Navigation in Rückwärtsrichtung.

- ToDo**
- Klicken Sie im Windows-Startmenü auf **Programme** ➤ **BRICKware** ➤ **Gerät an COM1** (bzw. **Gerät an COM2**, wenn Sie die COM2-Schnittstelle des Rechners benutzen), um **HyperTerminal** zu starten.
 - Drücken Sie die **Eingabetaste** (evtl. mehrmals), wenn sich das **HyperTerminal**-Fenster geöffnet hat.
Es erscheint ein Fenster mit dem Login-Prompt. Sie befinden sich auf der SNMP-Shell von **X1000**.
 - Fahren Sie fort mit [Kapitel 5.2, Seite 118](#).



Falls der Login-Prompt auch nach mehrmaligem Betätigen der **Eingabetaste** nicht erscheint, konnte die Verbindung zu **X1000** nicht hergestellt werden. Überprüfen Sie daher die Einstellungen von COM1 bzw. COM2:

- Klicken Sie auf **File** ➤ **Properties**.
- Klicken Sie im Register **Connect to** auf **Configure....**
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 **Settings** ein:
 - Emulation: VT100
- Klicken Sie auf **OK**.

Damit Änderungen an den Terminal-Programmeinstellungen wirksam werden, müssen Sie die Verbindung zu **X1000** trennen und wieder neu herstellen.



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

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.

5.1.2 Zugang über LAN



Über den Dienst >> **Telnet** können Sie **X1000** vom LAN aus erreichen. Telnet steht normalerweise auf jedem Rechner zur Verfügung. Um Ihren Router über das LAN erreichen zu können, muß er bereits eine >> **IP-Adresse** und >> **Netzmaske** haben. Wenn dies nicht der Fall ist, **X1000** also noch unkonfiguriert ist, haben Sie zwei Möglichkeiten:

- Wenn Sie mit Windows arbeiten, können Sie **X1000** eine IP-Adresse zuweisen, bevor Sie Telnet ausführen. Dazu benötigen Sie das Hilfsprogramm >> **DIME Tools**. Wenn Sie DIME Tools zusammen mit der **BRICKware for Windows** noch nicht installiert haben, gehen Sie vor wie in [Kapitel 3.3, Seite 47](#) beschrieben.
- Wenn Sie nicht mit Windows arbeiten, verwenden Sie für die Initialkonfiguration einen anderen Zugang (über die serielle Schnittstelle oder über ISDN).

ToDo > Schließen Sie **X1000** an das LAN an wie in [Kapitel 3.1, Seite 37](#) beschrieben.

IP-Adresse zuweisen Gehen Sie folgendermaßen vor, um **X1000** 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 **X1000** noch unkonfiguriert ist.
- > Geben Sie in diesem Fenster unter **BRICK Parameter** Name und IP-Adresse von **X1000** ein (wenn Sie unsicher sind, beachten Sie [Kapitel 3.2, Seite 40](#)).
- > Klicken Sie auf **OK**.
- > Schließen Sie **DIME Tools**.

Telnet ausführen Bauen Sie nun mit Telnet eine Verbindung zu **X1000** auf:

- Windows**
- Klicken Sie im Windows-Startmenü auf **Ausführen...**
 - Geben Sie `telnet <IP-Adresse von X1000>` ein.
 - Klicken Sie auf **OK**.

Es erscheint ein Fenster mit dem Login-Prompt. Sie befinden sich auf der SNMP-Shell von **X1000**. Fahren Sie fort mit [Kapitel 5.2, Seite 118](#).

- Unix**
- Geben Sie `telnet <IP-Adresse von X1000>` in ein Terminal ein.
- Es erscheint ein Fenster mit dem Login-Prompt. Sie befinden sich auf der SNMP-Shell von **X1000**. Fahren Sie fort mit [Kapitel 5.2, Seite 118](#).

Configuration Manager Der **Configuration Manager** greift ebenfalls über das LAN auf **X1000** zu. Die Kommunikation zwischen PC und **X1000** findet über das SNMP-Protokoll statt.

5.1.3 Zugang über ISDN

Remote-Konfiguration Der Zugang über **ISDN** mit **ISDN-Login** empfiehlt sich vor allem dann, wenn **X1000** sich an einem anderen Standort befindet, und Sie ihn aus der Ferne konfigurieren oder warten wollen. Dies ist auch dann möglich, wenn **X1000** sich noch im Auslieferungszustand befindet. Sie müssen dazu über einen anderen, bereits konfigurierten BinTec-Router (in LAN 1) verfügen und die Rufnummer Ihres (neuen) Routers (in LAN 2) kennen. So kann z. B. der Administrator in der Firmenzentrale den Router eines Mitarbeiters im Home Office konfigurieren, ohne vor Ort zu sein. **X1000** im Home Office muß lediglich mit dem ISDN-Anschluß verbunden und eingeschaltet sein.



Der Zugang über ISDN verursacht Kosten. Wenn **X1000**, Router und Rechner im gleichen LAN sind, ist es billiger, auf **X1000** über das LAN oder über die serielle Schnittstelle zuzugreifen.

- Schließen Sie **X1000** an das ISDN an wie in [Kapitel 3.1, Seite 37](#) beschrieben.

Gehen Sie folgendermaßen vor, um **X1000** über ISDN-Login zu erreichen:

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

- Geben Sie in der SNMP-Shell `isdnlogin <Rufnummer von X1000>` ein.

Es erscheint der Login-Prompt. Sie befinden sich auf der SNMP-Shell von **X1000**. Fahren Sie fort mit [Kapitel 5.2, Seite 118](#).

5.2 Anmelden

Unabhängig davon, über welchen Weg Sie auf **X1000** zugreifen, erscheint immer zunächst die **SNMP-Shell** von **X1000** mit dem Login-Prompt. (Eine Ausnahme bilden hier der Configuration Wizard und der Configuration Manager unter Windows.)

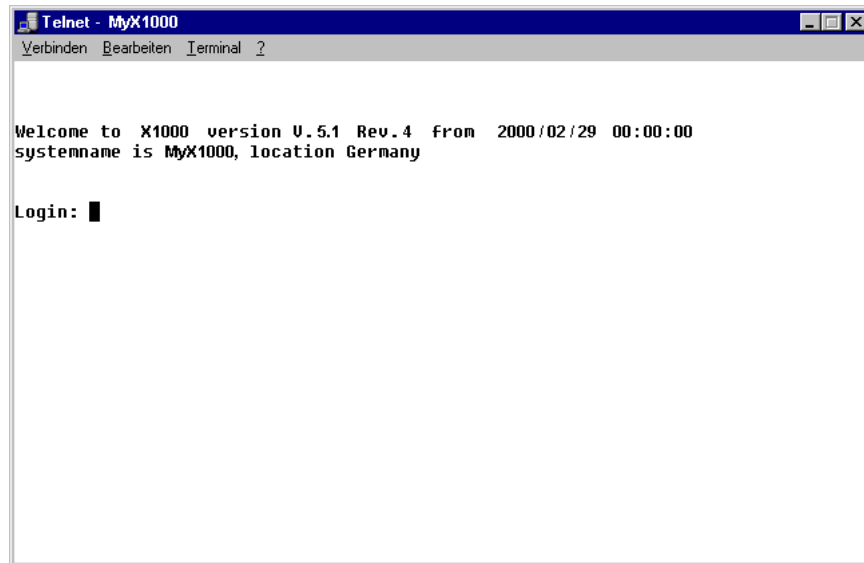


Bild 5-2: Login-Prompt

Um sich einloggen zu können, müssen Sie Benutzernamen und Paßwort kennen. Im Auslieferungszustand ist **X1000** 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 X1000 verloren).
read	public	Systemvariablen lesen.
http	bintec	HTTP-Statusseite von X1000 aufrufen, Systemvariablen lesen, kein Einloggen.

Tabelle 5-1: Benutzernamen und Paßwörter im Auslieferungszustand

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

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 **X1000** 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.

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. `x1000:>`. Das Einloggen war erfolgreich.



Achtung!

Um unberechtigten Zugriff auf **X1000** zu verhindern, sollten Sie gleich als erstes die Paßwörter ändern, falls Sie dies nicht schon bei der Grundkonfiguration mit dem Configuration Wizard getan haben.

- Ändern Sie die Paßwörter, wie in [Kapitel 6.1.2, Seite 140](#) beschrieben.

SNMP-Shell schließen

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

5.3 Konfigurationsmöglichkeiten

Bevor Sie mit der Konfiguration loslegen, müssen Sie sich für eine Methode entscheiden. Daher folgt hier zunächst eine Übersicht der verschiedenen Konfigurationsmöglichkeiten und eine Einführung in die Verwendung des Setup Tools. Anhand des Setup Tools beschreibt dieses Handbuch, wie Sie **X1000** konfigurieren.

5.3.1 Übersicht

Die Möglichkeiten, **X1000** zu konfigurieren:

- Configuration Wizard
- Setup Tool
- >> **SNMP**-Shell-Kommandos
- Configuration Manager
- Andere SNMP-Manager

Configuration Wizard Die Konfiguration mit dem Configuration Wizard haben Sie bereits in [Kapitel 3.5, Seite 55](#) kennengelernt. Sie dient zur schnellen Grundkonfiguration von **X1000** und kann genutzt werden, wenn Sie über einen Windows-PC verfügen. Standardkonfigurationen sind in der Regel damit abgedeckt. Wenn Sie aber darüberhinaus noch weitere Einstellungen benötigen, stehen Ihnen die anderen oben genannten Konfigurationsmöglichkeiten zur Verfügung. Sie können zunächst **X1000** 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 **X1000**. Die Konfiguration mit dem Setup Tool ist wesentlich einfacher und übersichtlicher als die Konfiguration mit SNMP-Kommandos, allerdings können nicht alle Einstellungen mittels Setup Tool vorgenommen werden. In diesem Handbuch wird neben dem Configuration Wizard ausschließlich das Setup Tool zur Konfiguration beschrieben. Das Setup Tool ist unabhängig vom

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

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

Configuration Manager und andere SNMP-Manager

Mit dem Configuration Manager stellt BinTec Communications AG einen SNMP-Manager für Windows-PCs zur Verfügung. In einer an den Microsoft Explorer angelehnten Oberfläche können Sie damit auf alle MIB-Tabellen und -Variablen (siehe [Kapitel 4.8, Seite 109](#)) von **X1000** zugreifen. Über andere SNMP-Manager, wie z. B. SNM, HP-Open View oder Transview, können Sie ebenfalls auf die MIB-Tabellen und MIB-Variablen zugreifen und sie ändern. Für den Umgang mit SNMP-Shell-Kommandos bzw. SNMP-Manager sind allerdings vertiefte Kenntnisse der Struktur und inneren Zusammenhänge von **X1000** erforderlich, die Methode ist also für erfahrene Nutzer interessant. Der Umgang mit MIB-Tabellen und MIB-Variablen wird in der Software Reference und MIB Reference erläutert.

5.3.2 Bedienung und Menüstruktur des Setup Tools

Wenn Sie sich auf **X1000** eingeloggt haben, können Sie das Setup Tool aufrufen:

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

Das Hauptmenü des Setup Tools erscheint.

Hauptmenü

X1000 Setup Tool		BinTec Communications AG	
		MyX1000	
Licenses		System	
LAN:	CM-100BT, Fast Ethernet		
WAN:	CM-1BRI, ISDN S0		
WAN Partner			
IP	IPX	PPP	ISDN CAPI
Configuration Management			
Monitoring and Debugging			
Exit			
Press <Ctrl-n>, <Ctrl-p> to scroll through menu items, <Return> to enter			



Das Hauptmenü des Setup Tools sieht unterschiedlich aus, je nachdem ob die Lizenzdaten bereits eingegeben sind oder nicht. Die Abbildung gilt für eine bereits eingetragene Standardlizenz.



Um das Setup Tool zu nutzen, müssen Sie sich mit dem Benutzernamen `admin` einloggen! Wenn Sie das entsprechende Paßwort nicht kennen, können Sie das Setup Tool nicht aufrufen (siehe [Kapitel 5.2, Seite 118](#)).

Das Setup Tool ist einfach zu bedienen. Sie werden sich darin sofort gut zurechtfinden. Dennoch sollten Sie sich zunächst mit den Möglichkeiten des Setup Tools vertraut machen. Es folgt zunächst eine Einführung in das Setup Tool von **X1000**.

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

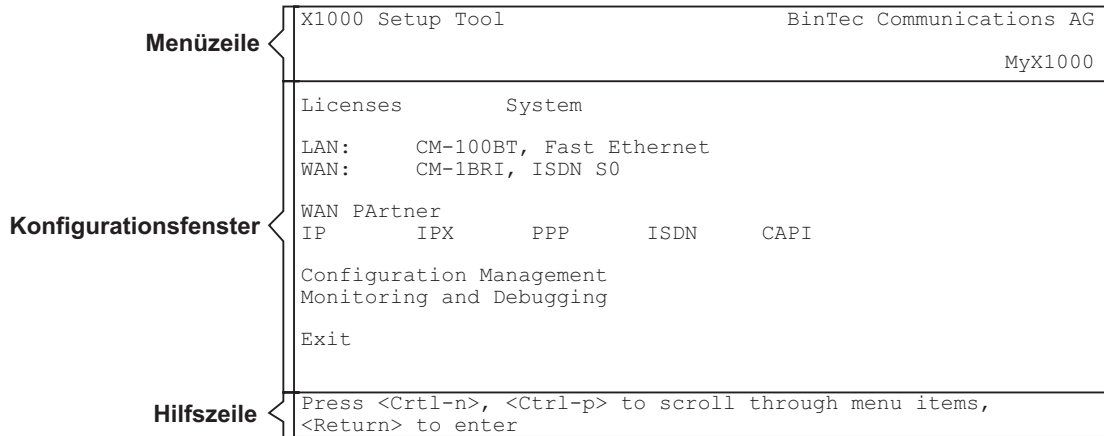


Bild 5-3: Setup-Tool-Menü-Layout

In der Menüzeile befindet sich eine Navigationshilfe, die anzeigt, in welchem Menü des Setup Tools Sie sich gerade befinden. Zusätzlich wird der Systemname von **X1000** 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 jeweils 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 ohne Speichern verlassen.

Tabelle 5-2: Navigation im Setup Tool

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

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

Tabelle 5-3: Schaltflächen im Setup Tool

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

```

X1000 Setup Tool                               BinTec Communications AG
[WAN]: WAN Partners                             MyX1000

Current WAN Partner Configuration

  Partnername      Protocol      State
  -----
  BigBoss          ppp          dormant
  T_ONLINE         ppp          dormant
  Partner1         ppp          dormant
  Partner2         ppp          dormant
  PROVIDER         ppp          dormant

ADD              DELETE          EXIT

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

```

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

Gehen Sie folgendermaßen vor:

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

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

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

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



Falls die Suche nicht funktioniert, stellen Sie sicher, daß sich der Cursor auf einem Listenelement befindet.

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

Beispiel:

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

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

Tabelle 5-4: Suchergebnisse

Paßwortänderung

Die im folgenden beschriebene Vorgehensweise zur Paßwortänderung betrifft alle Paßwörter auf **X1000**: die Zugangspaßwörter für die Benutzernamen `admin`, `read` und `write`, das HTTP-Paßwort, das PPP-Paßwort und das Provider-Paßwort.

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



Um das Setup Tool von **X1000** 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 **X1000** 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.
- Wiederholen Sie die Paßworteingabe und bestätigen Sie 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.

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

MENÜ ➤ **UNTERMENÜ** ➤ **UNTERMENÜ**

Beispiele:

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

im Menü WAN Partner den entsprechenden WAN-Partner und bestätigen Sie mit der Eingabetaste." Dies wird dargestellt als:

Gehen Sie zu **WAN PARTNER** ► **EDIT** ► **WAN NUMBERS**.

Menüstruktur Die Menüstruktur des Setup Tools sieht folgendermaßen aus:

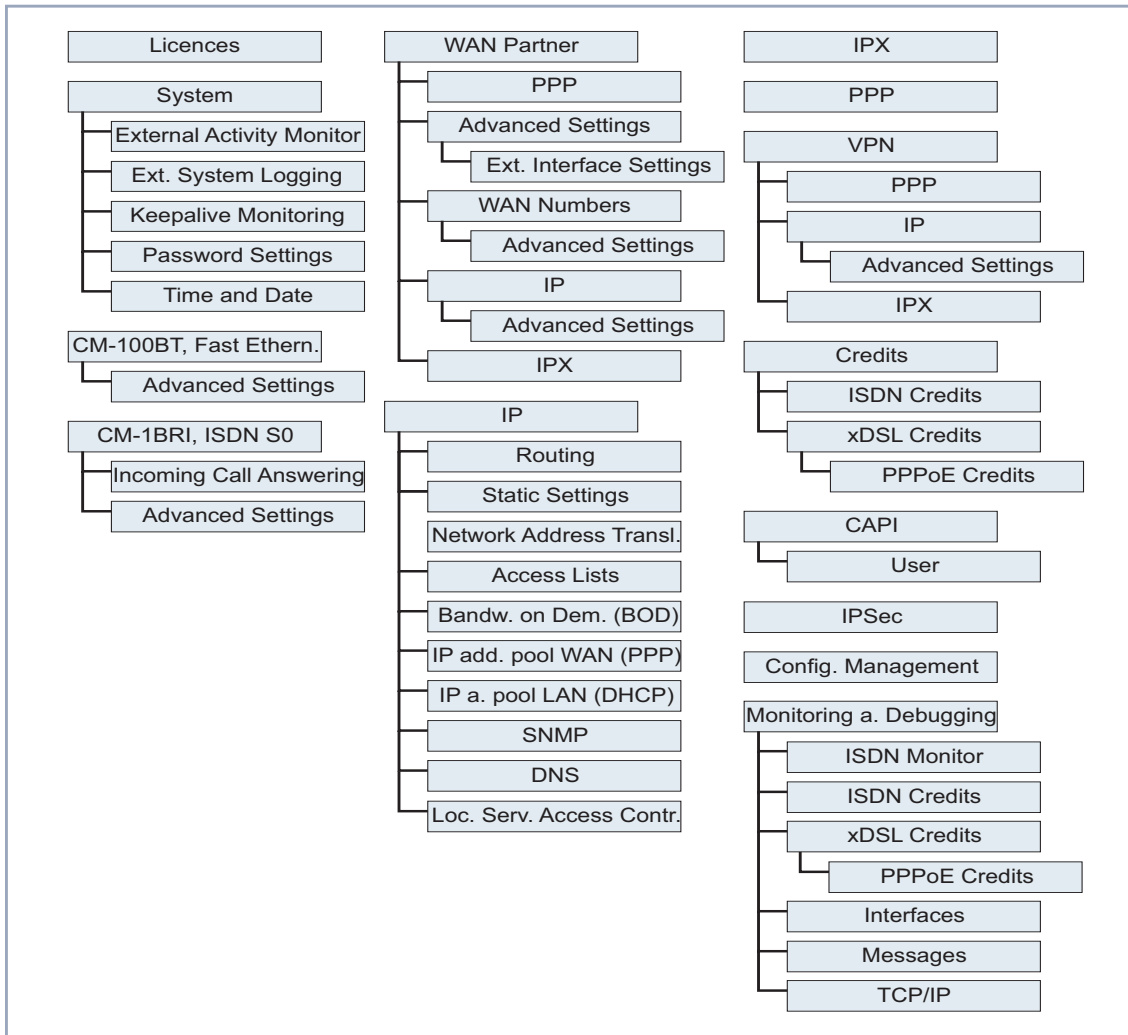


Bild 5-4: Setup-Tool-Menüstruktur

Bild 5-4, Seite 130 stellt alle auf **X1000** zur Verfügung stehenden Menüs des Setup Tools dar. Nicht alle Funktionen stehen auf jedem Router zur Verfügung (z. B. VPN). Um sie nutzen zu können, benötigen Sie eine Zusatzlizenz, die Sie bei BinTec Communications AG erwerben können. Wenn Sie die erforderliche Lizenz aktivieren, erkennt dies **X1000** und zeigt die entsprechenden Menüs an (Lizenz eintragen siehe Kapitel 6.1.1, Seite 138).

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

Menü	Funktion
LICENSES	In diesem Menü tragen Sie die Lizenzinformationen ein, die auf der mitgelieferten Lizenzkarte vermerkt sind. Hier aktivieren Sie auch die Zusatzlizenzen.
SYSTEM	In diesem Menü tragen Sie die grundlegenden Systemeinstellungen von X1000 ein, wie z. B. Systemname und Paßwörter.
CM-100BT, FAST ETHER-NET	In diesem Menü konfigurieren Sie die ►► LAN-Schnittstelle von X1000 . Hier tragen Sie z. B. die IP-Adresse und Netzmaske von X1000 ein.
CM-1BRI, ISDN S0	In diesem Menü konfigurieren Sie die ►► WAN-Schnittstelle von X1000 . Hier tragen Sie z. B. ein, an welcher Art von ISDN-Anschluß X1000 angeschlossen ist. Im Untermenü WAN INTERFACE ► INCOMING CALL ANSWERING teilen Sie die zur Verfügung stehenden ISDN-Rufnummern den gewünschten Diensten (z. B. PPP-Routing, ►► CAPI, ►► ISDN-Login) zu.
WAN PARTNER	In diesem Menü definieren Sie alle WAN-Partner, z. B. Ihren ►► Internet Service Provider (►► ISP). 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 X1000. Hier tragen Sie Routen zu Ihren Partnern ein (z. B. Default-Routen, Netzwerkrouuten), damit X1000 alle Datenpakete an die richtigen Adressen weiterleitet.</p> <p>In IP ► STATIC SETTINGS tragen Sie einige wichtige Einstellungen ein, z. B. den Domain Name von X1000, 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 X1000 ungewollt Verbindungen zum ISDN aufbaut.</p> <p>In IP ► IP ADDRESS POOL WAN (PPP) können Sie einen Pool von IP-Adressen einrichten, die X1000 als dynamischer IP Address Server an WAN-Partner vergibt, die sich einwählen.</p> <p>In IP ► IP ADDRESS POOL LAN (DHCP) konfigurieren Sie X1000 als DHCP Server. Als DHCP Server teilt X1000 den Hosts im LAN deren IP-Adressen dynamisch zu.</p> <p>In IP ► SNMP ändern Sie die grundlegenden SNMP-Einstellungen.</p> <p>In IP ► DNS können Sie die Vorgehensweise bei der Namensauflösung auf X1000 festlegen.</p> <p>In IP ► TOKEN AUTHENTICATION FIREWALL authentisieren Sie IP-Verbindungspartner personenbezogen.</p> <p>In IP ► LOCAL SERVICES ACCESS CONTROL kann der Zugang zu den lokalen UDP- bzw. TCP-Diensten auf X1000 geregelt werden.</p>

Menü	Funktion
IPX	In diesem Menü nehmen Sie die Eintragungen vor, die das IPX-Protokoll betreffen. ►► IPX wird vor allem in Novell-Netzwerken verwendet.
PPP	Enthält allgemeingültige ►► PPP -Einstellungen, z. B. Authentication Protocol, die sich nicht nur auf einzelne WAN-Partner beziehen. Der Router führt mit diesen Einstellungen eine Authentisierungsverhandlung mit eingehenden Rufen aus, wenn er die Calling Line Number nicht identifizieren kann (z. B. weil der Anruf über eine analoge Leitung eingeht, die die Calling Line Number nicht transportiert).
VPN	In diesem Menü nehmen Sie die nötigen Einstellungen für Virtual Private Networking (VPN) vor. Es erscheint nur, wenn Sie eine dafür gültige Lizenz eingetragen haben. Die Lizenz können Sie optional erwerben. Detaillierte Erklärungen und Hinweise zur Konfiguration finden Sie in der Software Reference.
CREDITS	In diesem Menü verwalten Sie die Taschengeldkonten (Credits Based Accounting System) von X1000 .
CAPI	Enthält die Einstellungen für das ►► CAPI User Concept von BinTec. Damit können Sie an Nutzer der CAPI-Anwendungen von X1000 Benutzernamen und Paßwörter vergeben. So stellen Sie sicher, daß nur autorisierte Nutzer eingehende Rufe empfangen und ausgehende Verbindungen via CAPI aufbauen können.
IPSEC	In diesem Menü nehmen Sie die nötigen Einstellungen für Internet Protocol Security (IPSec) vor. Es erscheint nur, wenn Sie eine dafür gültige Lizenz eingetragen haben. Die Lizenz können Sie optional erwerben. Detaillierte Erklärungen und Hinweise zur Konfiguration finden Sie im IPSec Reference Manual, das zusammen mit der Lizenz ausgeliefert wird, oder in der Software Reference.
CONFIGURATION MANAGEMENT	In diesem Menü verwalten Sie die Konfigurationsdateien von X1000 . Sie speichern Sie z. B. lokal auf X1000 oder aber auf Ihrem Rechner ab.
MONITORING AND DEBUGGING	Enthält Untermenüs, die das Auffinden von Problemen in Ihrem Netzwerk und das Überwachen von Aktivitäten auf X1000 , ermöglichen.

Menü	Funktion
<i>EXIT</i>	<p>Mit Exit verlassen Sie das Setup Tool.</p> <p>Mit Exit ► Save as boot configuration and exit speichern Sie die Konfigurationsdatei im Flash-Speicher, nach einem Restart von X1000 wird diese Datei geladen.</p> <p>Mit Exit ► Exit without saving gehen alle Änderungen nach dem nächsten Hochfahren von X1000 verloren.</p>

Tabelle 5-5: Menüs im Setup Tool

6 Grundkonfiguration mit dem Setup Tool

Die Grundkonfiguration von **X1000** mit dem **Setup Tool** beinhaltet die gleichen Themen wie die Konfiguration mit dem Configuration Wizard in [Kapitel 3.5, Seite 55](#). Allerdings ist das Setup Tool unabhängig vom Betriebssystem und Sie können zusätzlich weitere Einstellungen vornehmen.

Grundkonfiguration Die Grundkonfiguration von **X1000** umfaßt:

- Die grundlegenden **Router-Einstellungen**
- Das Einrichten von **WAN-Partnern**
 - für Internet-Zugang
 - für LAN-LAN-Kopplung (z. B. Firmennetzanbindung)
- Das Sichern der Konfigurationsdatei

Die grundlegenden Router-Einstellungen sind für das Funktionieren von **X1000** unbedingt erforderlich. Den Internet-Zugang und die Firmennetzanbindung können Sie je nach Bedarf gleich einrichten oder später hinzufügen.

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

- wie Sie einen weiteren **WAN-Partner** hinzufügen.
- wie Sie die Paßwörter ändern.
- wie Sie eine Zusatzlizenz eintragen.
- wie Sie das Verteilen der eingehenden Anrufe (Incoming Call Answering) organisieren.
- wie Sie **X1000** als **DHCP** Server einrichten.
- wie Sie einen einfachen **NetBIOS-Filter** definieren.
- wie Sie Routing-Einträge erstellen.

Wie Sie weitere Konfigurationsschritte nach Abschluß der Grundkonfiguration durchführen, finden Sie in [Kapitel 7, Seite 213](#).

Wie Sie Sicherheitsmechanismen gemäß SAFERNET einrichten, finden Sie in [Kapitel 8, Seite 307](#).



Nutzen Sie die Funktion Taschengeldkonto (siehe [Kapitel 8.1.3, Seite 317](#)). Damit können Sie für Verbindungen mit **X1000** ein Limit festlegen, um Gebühren aufgrund von Fehlern bei der Konfiguration in Grenzen zu halten.

6.1 Grundlegende Router-Einstellungen

Das Einrichten der grundlegenden Router-Einstellungen betrifft nur **X1000** und Ihr lokales Netzwerk. In [Bild 6-1, Seite 137](#) ist der relevante Ausschnitt aus [Bild 6-4, Seite 169](#) abgebildet. Dort sind beispielhaft Namen, **IP-Adressen**, Rufnummern, etc. angegeben. Wenn Sie ein neues lokales Netzwerk (LAN) zusammen mit **X1000** einrichten und keine IP-Adressen zugeteilt bekommen haben (z. B. von Ihrem Systemadministrator in der Firmenzentrale), sollten Sie als IP-Adressen einfach die Beispielwerte übernehmen.

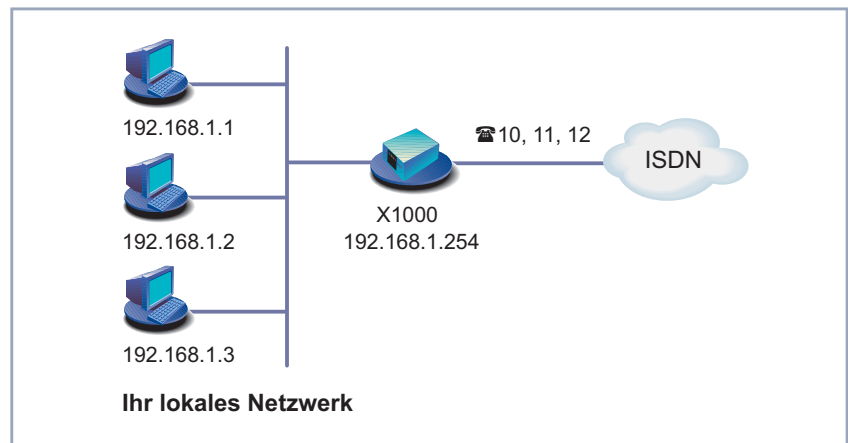


Bild 6-1: Grundlegende Router-Einstellungen

Folgende Schritte sind erforderlich:

- Lizenzen eintragen
- Systemdaten (z. B. Paßwörter) eintragen
- LAN-Schnittstelle konfigurieren
- **WAN-Schnittstelle** konfigurieren
- **X1000** als DHCP **Server** einrichten (optional)
- **Filter** setzen (optional, ausführlich in [Kapitel 8.2.8, Seite 338](#))

Los geht's!

6.1.1 Lizenzen eintragen

Lizenzkarte Nachdem Sie sich wie in [Kapitel 5.2, Seite 118](#) beschrieben auf **X1000** 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 **X1000** frei.

➤ Gehen Sie zu **LICENSES**:

```

X1000 Setup Tool                               BinTec Communications AG
[LICENSE]: Licenses                             MyX1000

Available Licenses:

IP (builtin), STAC (valid), CAPI (valid), IPX (valid)

Serialnumber      Mask          Key          State
101546            5134         88PNUPZ     ok

ADD                DELETE                EXIT

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

```

Unter **Available Licenses** sind die auf **X1000** verfügbaren Subsysteme und deren Status (*builtin* - immer verfügbar, *valid* - freigeschaltet) aufgelistet.

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

Wenn Sie noch keine Lizenz eingetragen haben, ist in der Subsystem-Liste nur **IP** eingetragen, d.h. ➤➤ **IP-Routing** ist verfügbar (*builtin*).

Subsysteme Folgende Subsysteme stehen prinzipiell auf **X1000** zur Verfügung:

Subsysteme	Bedeutung
IP	IP-Routing.
TUNNEL	Virtual Private Networking VPN (nur mit Zusatzlizenz).
LEASED LINE	Festverbindung (nur mit Zusatzlizenz).
STAC	➤➤ STAC -➤➤ Datenkompression .
CAPI	➤➤ Remote-CAPI -Schnittstelle, ermöglicht Kommunikationsanwendungen auf Ihrem Rechner, z. B. Faxe versenden und empfangen.
IPX	➤➤ IPX -Routing.
IPSEC	Internet Protocol Security (nur mit Zusatzlizenz).

Tabelle 6-1: Subsysteme

ToDo Gehen Sie folgendermaßen vor, um eine Lizenz einzutragen:

- Fügen Sie einen neuen Eintrag mit **ADD** hinzu.
Ein weiteres Menüfenster erscheint.
- Geben Sie **Serial Number** ein.
- Geben Sie **Mask** ein.
- Geben Sie **Key** ein.
- Bestätigen Sie mit **SAVE**.
Sie befinden sich wieder im Menü **LICENSES**. Die mit Ihrer Lizenz freigeschalteten Subsysteme sind aufgelistet. 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.

6.1.2 Systemdaten eintragen

Systemname, ... Tragen Sie als nächstes die grundlegenden Systemdaten zur Identifikation von **X1000** ein.

➤ Gehen Sie zu **SYSTEM:**

X1000 Setup Tool	BinTec Communications AG
[SYSTEM]: Change System Parameters	MyX1000
System Name	MyX1000
Local PPP ID (default)	LittleIndian
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 X1000 , wird auch als PPP-Host-Name benutzt. Erscheint beim Einloggen auf X1000 als Eingabeprompt. 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 X1000 nötig, wenn eine nicht-partnerspezifische PPP-Authentisierung (z. B. PAP oder CHAP) durchgeführt wird (siehe Kapitel 7.1.3, Seite 220).
Location	(optional) Gibt an, wo sich X1000 befindet.
Contact	(optional) Gibt die zuständige Kontaktperson an. Wenn die Person von der HTTP-Statusseite von X1000 aus erreichbar sein soll, muß hier eine gültige E-Mail-Adresse eingetragen werden.

Tabelle 6-2: **SYSTEM**

Paßwörter Im Untermenü **SYSTEM** ➤ **PASSWORD SETTINGS** geben Sie die Paßwörter für **X1000** 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 X1000 .

Tabelle 6-3: **SYSTEM** ➤ **PASSWORD SETTINGS**



Achtung!

Alle BinTec-Router werden mit gleichem Benutzernamen und Paßwort ausgeliefert. Sie sind daher nicht gegen einen unautorisierten Zugriff geschützt, solange die Paßwörter nicht geändert wurden. Die Vorgehensweise bei der Änderung von Paßwörtern ist unter "[Paßwortänderung](#)", [Seite 128](#) beschrieben.

- Ändern sie unbedingt die Paßwörter, um unberechtigten Zugriff auf **X1000** zu verhindern.

Die Befugnisse der möglichen Benutzernamen und Paßwörter finden Sie in [Kapitel 5.2, Seite 118](#).

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

- Geben Sie **System Name** von **X1000** ein, z. B. **MyX1000**.
- 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 **X1000** mit dem Windows Tool Activity Monitor überwachen zu können (siehe [Kapitel 8.1.5, Seite 325](#) bzw. BRICKware for Windows).

Im Menü **SYSTEM** ► **EXTERNAL SYSTEM LOGGING** finden Sie Einstellungen für Syslog Messages (siehe [Kapitel 8.1.1, Seite 308](#)).

Im Menü **SYSTEM** ► **KEEPALIVE MONITORING** finden Sie Einstellungen für die Funktion Keepalive Monitoring (siehe [Kapitel 7.2.11, Seite 263](#)).

Im Menü **SYSTEM** ► **TIME AND DATE** finden Sie Einstellungen zur manuellen Eingabe von Uhrzeit und Datum auf **X1000** (siehe [Kapitel 7.3.1, Seite 269](#)).

6.1.3 LAN-Schnittstelle konfigurieren

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

Konfigurieren Sie als nächstes die LAN-Schnittstelle von **X1000**. 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 **X1000** 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:

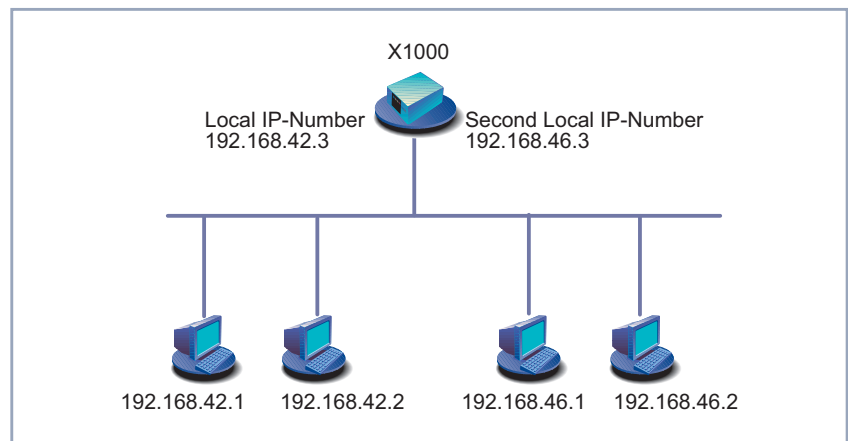


Bild 6-2: **X1000** mit zwei verschiedenen lokalen IP-Adressen

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 **X1000** 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.



Möglicherweise haben Sie **X1000** schon vor der Grundkonfiguration seine IP-Adresse und Netzmaske zugewiesen, z. B. mit Hilfe des **BootP Servers** der **DIME Tools**. Überprüfen Sie trotzdem die Eintragungen im folgenden Menü.

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

```

X1000 Setup Tool                               BinTec Communications AG
[LAN]: Configure Ethernet Interface             MyX1000

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- und **IPX**-Konfiguration möglich. In diesem Kapitel wird nur die Konfiguration von **IP** erläutert. Belassen Sie die unter **IPX Configuration** voreingestellten Werte.

Wenn Sie das **Protokoll IPX** verwenden, finden Sie Erläuterungen zur Konfiguration der LAN-Schnittstelle für IPX in [Kapitel 7.4, Seite 298](#).

Folgende Teile des Menüs sind für diesen Konfigurationsschritt interessant:

Feld	Bedeutung
local IP-Number	IP-Adresse von X1000 im LAN.
local Netmask	Netzmaske des Netzwerkes, in dem sich X1000 befindet.
Second Local IP-Number	Zweite IP-Adresse von X1000 im LAN.
Second Local Netmask	Netzmaske des Teilnetzwerks, in dem sich X1000 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>Im allgemeinen können Sie den Standardwert <i>Ethernet II</i> belassen. Mit <i>Ethernet II</i> heißt die LAN-Schnittstelle <i>en1</i>, mit <i>Ethernet SNAP</i> <i>en1-snap</i>.</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>

Tabelle 6-4: **CM-BNC/TP, ETHERNET**

ToDo Gehen Sie folgendermaßen vor, um die LAN-Schnittstelle von **X1000** zu konfigurieren:

- Geben Sie **local IP-Number** von **X1000** 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.

6.1.4 WAN-Schnittstelle konfigurieren

Schnittstelle zum ISDN Konfigurieren Sie als nächstes die ➤➤ **WAN-Schnittstelle** von **X1000**. Die WAN-Schnittstelle ist die physikalische Schnittstelle zum ➤➤ **ISDN**. Sie können sie für Wählverbindungen und mit Zusatzlizenz auch für Festverbindungen nutzen. Um sie zu konfigurieren, müssen Sie für Wählverbindungen zwei Schritte durchführen:

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

Autokonfiguration, ISDN Switch Type, ... Machen Sie zunächst die Einstellungen für Ihren ISDN-Anschluß.

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

```
X1000 Setup Tool                               BinTec Communications AG
[WAN]: WAN Interface                             MyX1000

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 -Protokoll-Erkennung läuft, bis eine Einstellung gefunden wird bzw. bis das ISDN-Protokoll unter ISDN Switch Type manuell eingegeben ist. Festverbindungen müssen unter ISDN Switch Type immer manuell eingestellt werden.

Feld	Bedeutung
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-Kanal-Protokoll-Erkennung (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>: ISDN-Anschluß deaktiviert■ <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 <p>Die Einstellungen für Festverbindungen (leased lines) erscheinen nur, wenn Sie eine entsprechende Lizenz eingetragen haben.</p>

Feld	Bedeutung
D-Channel	<p>Konfiguration des D-Kanals. Eine Veränderung der Auswahl ist nur möglich bei ISDN Switch Type = leased line D + B1 + B2 (TS02). Auswählbare Werte:</p> <ul style="list-style-type: none"> ■ <i>leased dte</i> (Standardwert) ■ <i>leased dce</i>
B-Channel 1	<p>Konfiguration des ersten ➤➤ B-Kanals. Auswählbare Werte:</p> <ul style="list-style-type: none"> ■ <i>dialup</i> (Standardwert) ■ <i>not used</i> ■ <i>leased dte</i> ■ <i>leased dce</i> <p>Die Einstellungen für Festverbindungen (leased line) erscheinen nur, wenn Sie eine entsprechende Lizenz eingetragen haben.</p>
B-Channel 2	<p>Konfiguration des zweiten B-Kanals. Auswählbare Werte:</p> <ul style="list-style-type: none"> ■ <i>dialup</i> (Standardwert) ■ <i>not used</i> ■ <i>leased dte</i> ■ <i>leased dce</i> <p>Die Einstellungen für Festverbindungen (leased line) erscheinen nur, wenn Sie eine entsprechende Lizenz eingetragen haben.</p>

Tabelle 6-5: **CM-1BRI, ISDN S0**



Vermeiden Sie für Wählverbindungen unter **B-Channel 1** bzw. **B-Channel 2** die Einstellung *not used*, da dieser Modus unerwünschte Randeffekte nach sich ziehen kann.

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

- Wählen Sie **ISDN Switch Type** aus: *autodetect on bootup*.
Mit dieser Einstellung nutzt **X1000** die automatische D-Kanal-Erkennung. Unter **Result of Autoconfiguration** erscheint *running*, solange die D-Kanal-Erkennung läuft. Danach wird die gefundene Einstellung angezeigt, z. B. *Euro ISDN, point to multipoint*.



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

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

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



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 (siehe [Kapitel 7.5.3, Seite 305](#)) 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).

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

Incoming Call Answering Falls Sie die WAN-Schnittstelle für Wählverbindungen verwenden, müssen Sie als nächstes **X1000** mitteilen, wie auf eingehende Rufe aus dem ISDN reagiert bzw. wie mit ausgehenden Rufen verfahren werden soll. (Für Festverbindun-

gen sind diese Einstellungen nicht erforderlich.) Entsprechend den Einstellungen in den folgenden Menüs verteilt **X1000** die eingehenden Rufe auf die internen Dienste.

X1000 unterstützt die Dienste:

■ PPP (Routing)

Der Dienst >>> **PPP** ist der allgemeine Routing-Dienst von **X1000**. 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.

■ ISDN-Login

Der Dienst >>> **ISDN-Login** ermöglicht eingehenden Datenrufen Zugang zur >>> **SNMP-Shell** von **X1000**. So kann **X1000** aus der Ferne konfiguriert und gewartet werden.

■ CAPI

Der Dienst >>> **CAPI** ermöglicht eingehenden Daten- und Sprach-Rufen eine Verbindung mit Kommunikationsanwendungen auf Hosts im LAN, die auf die >>> **Remote-CAPI-Schnittstelle** von **X1000** zugreifen. So können beispielsweise mit **X1000** verbundene Hosts Faxe empfangen.

Wenn ein Ruf eingeht, überprüft **X1000** 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 **X1000** zu erreichen. Anschließend wird

der Ruf an den passenden Dienst weitergeleitet (siehe auch [Bild 6-3](#), [Seite 153](#)).

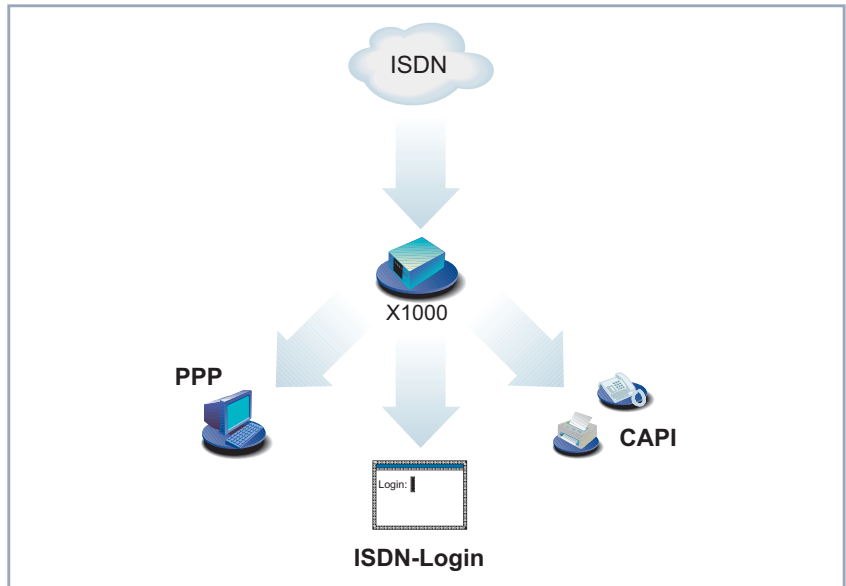


Bild 6-3: Verteilung der eingehenden Rufe auf Dienste

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

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

Tabelle 6-6: Verteilung der Rufnummern auf Dienste



Wenn Sie im folgenden Menü keine Eintragungen vornehmen, wird jeder 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.



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



Ordnen Sie Ihre eigenen Rufnummern den unterschiedlichen Diensten zu. Geben Sie daher unter **Number** Ihre eigenen Rufnummern ein.

Machen Sie nun die Eintragungen für Incoming Call Answering:

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

X1000 Setup Tool		BinTec Communications AG	
[WAN][INCOMING]: Incoming Call Answering		MyX1000	
Item	Number	Mode	Username
CAPI 1.1 EAZ 1 Mapping	11	right to left	
CAPI 1.1 EAZ 1 Mapping	11	right to left	
ISDN Login	12	right to left	
PPP (routing)	10	right to left	
ADD	DELETE	EXIT	
Press <Ctrl-n>, <Ctrl-p> to scroll, <Space> tag/untag DELETE, <Return> to edit			

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

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

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

Ein weiteres Menüfenster erscheint:

X1000 Setup Tool		BinTec Communications AG	
[WAN][INCOMING][ADD]:Incoming Call Answering		MyX1000	
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.
Number	Rufnummer, unter der der oben eingetragene Dienst (Item) erreicht werden kann.
Mode	<p>Modus, mit dem X1000 den Ziffernvergleich von Number mit der Called Party Number des eingehenden Rufes durchführt:</p> <ul style="list-style-type: none"> ■ <i>right to left</i> (Standardwert) ■ <i>left to right (DDI)</i>: Immer auswählen, wenn X1000 mit einem Point-to-Point-Anschluß (Anlagenanschluß) verbunden ist.
Username	CAPI-Benutzername. Nur erforderlich, wenn Sie das CAPI User Concept nutzen wollen (siehe Kapitel 7.1.2, Seite 216).
Bearer	<p>Art des eingehenden Rufes. Mögliche Werte:</p> <ul style="list-style-type: none"> ■ <i>data</i>: Datenruf ■ <i>voice</i>: Sprach-Ruf ■ <i>any</i>: sowohl Daten- als auch Sprach-Ruf

Tabelle 6-7: **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 kBit/s PPP-Datenverbindungen.
<i>PPP 56k</i>	Ermöglicht 56 kBit/s PPP-Datenverbindungen.
<i>PPP Modem</i>	Auf X1000 nicht verfügbar.
<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 Bit/s, 2400 Bit/s,..., 38400 Bit/s.
<i>Pots</i>	Auf X1000 nicht verfügbar.
<i>PPP Modem Profile 1...8</i>	Auf X1000 nicht verfügbar.
<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>	Auf X1000 nicht verfügbar.

Tabelle 6-8: **Item**

ToDo Machen Sie folgende Eintragungen:

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

- Bestätigen Sie mit **SAVE**.

Sie befinden sich wieder im Menü **CM-1BRI, ISDN 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 Datenruf an die Called Party Number 10 eingeht, wird er an den Dienst PPP (routing) weitergeleitet.



Da **X1000** alle eingehenden Rufe, die zu keinem Eintrag in diesem Menü passen, an den Dienst ➤➤ **CAPI** weiterleitet, ist es nicht unbedingt erforderlich, CAPI einzutragen (außer für CAPI 1.1-Anwendungen)!

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

Damit haben Sie Incoming Call Answering konfiguriert, **X1000** verteilt die eingehenden Rufe an die internen Dienste. Für ausgehende Rufe werden ebenfalls diese Rufnummern mit den zugeordneten Diensten verwendet.



Achten Sie darauf, unter **Number** die richtige Nummer, d. h. die Nummer, die auch wirklich bei **X1000** ankommt, einzutragen! Wenn **X1000** z. B. an einer ➤➤ **TK-Anlage** angeschlossen ist, kommt nur die Nebenstellenummer bei **X1000** an.

Wenn Sie sich nicht sicher sind, welche Nummer bei **X1000** wirklich ankommt, gehen Sie folgendermaßen vor:

- Rufen Sie mit einem herkömmlichen Telefon **X1000** 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 **X1000** ankommt.
- Geben Sie diesen Anteil der Rufnummer in **CM-1BRI, ISDN SO** ➤ **INCOMING CALL ANSWERING** ➤ **ADD** unter **Number** ein.



Mit dem CAPI User Concept (siehe [Kapitel 7.1.2, Seite 216](#)) können Sie den Zugriff auf die CAPI-Dienste bestimmten Nutzern mit eigenen Paßwörtern vorbehalten.

Weiterführende Konfiguration

Unter **CM-1BRI, ISDN S0** ► **ADVANCED SETTINGS** finden Sie Einstellungen für X.31-TEI (siehe [Kapitel 7.2.4, Seite 233](#)).

Falls Sie eine X.31-Festverbindung nutzen (siehe [Kapitel 7.5.3, Seite 305](#)), können Sie mit dem Feature Bandwidth on Demand u. a. eine Backuplösung realisieren (siehe [Kapitel 7.2.3, Seite 226](#)). Wenn Sie diese Möglichkeit nutzen, wird bei Ausfall der Festverbindung eine Wählverbindung zum Verbindungspartner aufgebaut.

6.1.5 X1000 als DHCP Server einrichten

IP-Adressen im LAN

Jeder Rechner in Ihrem ►► LAN benötigt, wie auch **X1000**, eine eigene IP-Adresse. Wenn Sie **X1000** als ►► DHCP (Dynamic Host Configuration Protocol)-Server einrichten, vergibt er anfragenden Rechnern im LAN automatisch ►► IP-Adressen aus einem definierten IP-Adreß-Pool. Ein Rechner sendet einen Adreß-Request aus und erhält daraufhin seine IP-Adresse von **X1000** 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 **X1000** 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:**

X1000 Setup Tool	BinTec Communications AG
[IP][DHCP][ADD]: Add range of IP Addresses	MyX1000
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 X1000 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 6-9: **IP** ➤ **IP ADDRESS POOL LAN (DHCP)** ➤ **ADD**

ToDo Machen Sie folgende Eintragungen, um **X1000** als DHCP Server einzurichten:

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

- Geben Sie **IP Address** ein, z. B. **192.168.1.1**.
- Geben Sie **Number of consecutive addresses** ein, z. B. **8**.
- Geben Sie **Lease Time (Minutes)** ein, z. B. **120**.
- Geben Sie gegebenenfalls **MAC Address** ein.
- Geben Sie gegebenenfalls **Gateway** ein.
- Wählen Sie **NetBT Node Type** aus, z. B. *not specified*.
- Bestätigen Sie mit **SAVE**.
Sie befinden sich im Menü **IP** ➤ **IP ADDRESS POOL LAN (DHCP)**, wo die IP-Adreß-Pools aufgelistet sind. Die Eintragungen sind gespeichert.



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

6.1.6 Filter setzen

NetBIOS-Filter Wenn Sie in Ihrem lokalen Netzwerk mit Windows arbeiten, sollten Sie ➤➤ **NetBIOS-Filter** setzen, um Gebühren zu sparen. Dies verhindert, daß **X1000** Verbindungen z. B. zum Internet Service Provider (➤➤ **ISP**) aufbaut, um WINS Requests von Rechnern in Ihrem Netzwerk weiterzugeben. D. h. **X1000** fragt beim ISP nach, welcher ➤➤ **Hostname** einer IP-Adresse zugeordnet werden kann. Da der ISP WINS-Namen nicht auflösen kann, sind diese Verbindungen unnötig, kosten aber Gebühren.

Ausführliche Erläuterungen zum Thema ➤➤ **Filter** finden Sie in [Kapitel 8.2.8, Seite 338](#).

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 Filterkonfiguration über die serielle Schnittstelle oder ISDN-Login auf **X1000** zu.
- Wenn Sie über Telnet auf **X1000** zugreifen, wählen Sie im Menü **IP** ➤ **ACCESS LISTS** ➤ **INTERFACES** ➤ **EDIT** aus: **First Rule = none**.
- Gehen Sie zu **IP** ➤ **ACCESS LISTS** ➤ **FILTER** ➤ **ADD**:

X1000 Setup Tool		BinTec Communications AG
[IP][ACCESS][FILTER][ADD]: Configure IP Access Filter		MyX1000
Description	wrong_dns	
Index	1	
Protocol	udp	
Source Address		
Source Mask		
Source Port	specify	
Specify Port	137	
Destination Address		
Destination Mask		
Destination Port	specify	
Specify Port	53	
	SAVE	CANCEL
Enter string, max length = 48 chars		

ToDo Machen Sie folgende Eintragungen, um ein Filter 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**:

X1000 Setup Tool		BinTec Communications AG	
[IP][ACCESS][RULE][ADD]: Configure IP Access Rules		MyX1000	
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:

```

X1000 Setup Tool                               BinTec Communications AG
[IP][ACCESS][RULE]: Configure IP Access Rules   MyX1000

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

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

                ADD                DELETE                REORG                EXIT

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

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

```

X1000 Setup Tool                               BinTec Communications AG
[IP][ACCESS][INTERFACES]: Configure First Rule  MyX1000

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 **X1000** (**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 Router-Einstellungen ist abgeschlossen.

- Verlassen Sie das Hauptmenü mit **EXIT** und speichern Sie die erstellte Konfiguration mit **Save as boot configuration and exit**.

Die Einstellungen sind damit im Flash gespeichert und gehen beim Ausschalten von **X1000** nicht verloren (siehe [Kapitel 6.3, Seite 211](#)).

6.2 X1000 und das WAN

Wenn Sie die Konfigurationsschritte in [Kapitel 6.1, Seite 137](#) durchgeführt haben, ist **X1000** für Ihr **LAN** eingerichtet. Wenn Sie auch auf Hosts außerhalb Ihres LANs zugreifen wollen, z. B. um im **Internet** zu surfen, ist dieses Kapitel interessant für Sie.

Folgende Punkte werden behandelt:

■ Einrichten eines **WAN-Partners** allgemein:

Um mit **X1000** Verbindungen zu Netzwerken außerhalb Ihres LANs herstellen zu können, müssen Sie die gewünschten Verbindungspartner als WAN-Partner auf **X1000** einrichten. Dies gilt für ausgehende Verbindungen (**X1000** wählt sich bei einem WAN-Partner ein), für eingehende Verbindungen (ein WAN-Partner wählt sich bei **X1000** ein) und für Festverbindungen (siehe [Kapitel 7.5.3, Seite 305](#)). Wenn Sie einen Internet-Zugang herstellen wollen, müssen Sie Ihren Internet Service Provider (**ISP**) als WAN-Partner einrichten. Wenn Sie eine LAN-LAN-Kopplung aufbauen wollen, z. B. zwischen Ihrem LAN und dem LAN Ihrer Firmenzentrale (Firmennetzanbindung), müssen Sie das LAN der Firmenzentrale als WAN-Partner einrichten.

In [Kapitel 6.2.1, Seite 169](#), wird in allgemeiner Form erläutert, wie Sie vorgehen, um einen WAN-Partner auf **X1000** einzurichten.

Wenn Sie bei der Konfiguration der WAN-Schnittstelle von **X1000** eine oder zwei Festverbindungen am S₀-Anschluß eingerichtet haben (siehe [Kapitel 6.1.4, Seite 146](#)), erscheint im Menü WAN Partner automatisch jeweils ein WAN-Partner-Eintrag je Festverbindung. Editieren Sie diesen Eintrag entsprechend Ihren Erfordernissen.

■ Einrichten eines WAN-Partners für Zugang zum Internet (anhand von Beispielen):

In [Kapitel 6.2.2, Seite 195](#) finden Sie Beispiele für das Einrichten eines Internet Service Providers als WAN-Partner. Wenn Sie Ihren Internet-Zugang über einen der folgenden Provider ausführen, finden Sie dort eine schnelle Vorgehensweise, um mit **X1000** ins Internet zu gelangen:

- T-Online
- CompuServe

- Einrichten eines WAN-Partners zur Firmennetzanbindung (anhand von Beispielen):

In [Kapitel 6.2.3, Seite 201](#) finden Sie zwei Beispiele für das Einrichten einer Firmennetzanbindung. Das erste Beispiel erläutert die Anbindung einer Niederlassung an eine Firmenzentrale. In den meisten Fällen wird dieses Beispiel genügen. Im zweiten Beispiel erfahren Sie, wie Sie sich als Außendienstmitarbeiter oder als Mitarbeiter am Heimarbeitsplatz ohne Router in der Firmenzentrale einwählen können, d.h. wie **X1000** in der Firmenzentrale konfiguriert sein muß und was Sie an Ihrem PC tun müssen.

In [Bild 6-4, Seite 169](#) ist ein grundlegendes Szenario abgebildet, wie eine Verbindung von **X1000** zu den WAN-Partnern Internet Service Provider und Firmenzentrale aussehen könnte!

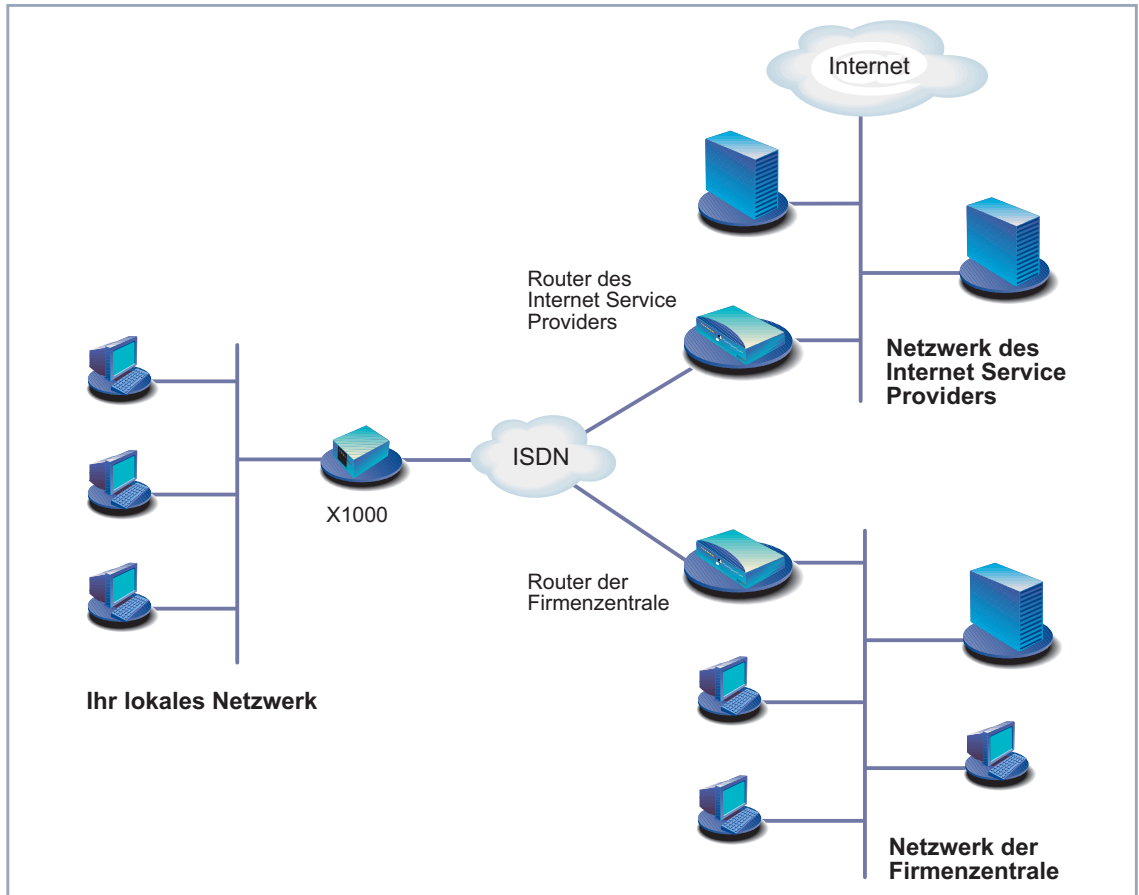


Bild 6-4: Grundszenario

6.2.1 WAN-Partner einrichten

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

- WAN-Partner eintragen:
 - >> **Protokoll** festlegen.
 - Rufnummer(n) eintragen.

- >>> **PPP**-Einstellungen zur Authentisierung festlegen.
- >>> **Shorthold** festlegen.
- IP-Konfiguration durchführen.

■ Routing-Eintrag erstellen

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

Los geht's!

WAN-Partner eintragen

WAN-Partner einrichten

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

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

➤ Gehen Sie zu **WAN PARTNER**:

X1000 Setup Tool	BinTec Communications AG	
[WAN]: WAN Partners	MyX1000	
Current WAN Partner Configuration		
Partnername	Protocol	State
T-Online	ppp	dormant
ADD	DELETE	EXIT
Press <Ctrl-n>, <Ctrl-p> to scroll, <Space> tag/untag DELETE, <Return> to edit		

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



Wenn Sie bei der Konfiguration der WAN-Schnittstelle von **X1000** eine oder mehrere Festverbindungen eingerichtet haben (siehe [Kapitel 6.1.4, Seite 146](#)), wird im Menü WAN Partner bereits automatisch jeweils ein WAN-Partner für eine Festverbindung angelegt. Editieren Sie diesen Eintrag entsprechend Ihren Erfordernissen.

State kann folgende Werte annehmen:

- *up*: verbunden
- *dormant*: nicht verbunden
- *blocked*: nicht verbunden (aufgrund eines Fehlers beim Verbindungsaufbau ist ein erneuter Versuch erst nach einer definierten Anzahl von Sekunden möglich, siehe [Kapitel 7.2.1, Seite 223](#))
- *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:

X1000 Setup Tool	BinTec Communications AG
[WAN][ADD]:Configure WAN Partner	MyX1000
Partner Name	T-Online
Encapsulation	PPP
Compression	none
Encryption	none
Calling Line Identification	no
PPP >	
Advanced Settings >	
WAN Numbers	
IP >	
IPX>	
SAVE	CANCEL
Enter string, max length = 25 chars	

Das Menü enthält folgende Felder:

Feld	Bedeutung
Partner Name	Geben Sie einen beliebigen Namen ein, um den WAN-Partner eindeutig zu benennen.
Encapsulation	<p>➤➤ Enkapsulierung. Definiert, wie die</p> <p>➤➤ Daten-Pakete für die Übertragung zum WAN-Partner verpackt werden. Mögliche Werte:</p> <ul style="list-style-type: none"> ■ <i>PPP</i> ■ <i>Multi-Protocol LAPB Framing</i> ■ <i>Multi-Protocol HDLC Framing</i> ■ <i>Async PPP over X.75</i> ■ <i>Async PPP over X.75/T.70/BTX</i> ■ <i>X.25_PPP</i>: auf X1000 nicht verfügbar ■ <i>X.25</i>: auf X1000 nicht verfügbar ■ <i>HDLC Framing (only IP)</i> ■ <i>LAPB Framing (only IP)</i> ■ <i>X31 B-Channel</i>: auf X1000 nicht verfügbar ■ <i>X.25 No Signalling</i>: auf X1000 nicht verfügbar ■ <i>X.25 PAD</i>: auf X1000 nicht verfügbar ■ <i>X.25 No Configuration</i>: auf X1000 nicht verfügbar ■ <i>Frame Relay</i>: auf X1000 nicht verfügbar ■ <i>X.25 No Configuration, No Signalling</i>: auf X1000 nicht verfügbar

Feld	Bedeutung
Compression	Legt die Art der Komprimierung fest, die für den Datenverkehr mit dem WAN-Partner angewendet werden soll. Mögliche Werte: <ul style="list-style-type: none"><li data-bbox="802 396 1245 427">■ <i>STAC</i>: nur bei Encapsulation = PPP<li data-bbox="802 447 1288 478">■ <i>MS-STAC</i>: nur bei Encapsulation = PPP<li data-bbox="802 498 902 529">■ <i>none</i>

Feld	Bedeutung
Encryption	<p>Definiert die Art der Verschlüsselung, die für den Datenverkehr mit dem WAN-Partner angewendet werden soll. Nur nutzbar, 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 128</i>: MPPE Version 1 mit 128-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>MPPE V2 128</i>: MPPE Version 2 mit 128-Bit-Schlüssel ■ <i>Blowfish 56</i>: Blowfish mit 56-Bit-Schlüssel ■ <i>Blowfish 168</i>: Blowfish mit 168-Bit-Schlüssel ■ <i>DES 56</i>: DES mit 56-Bit-Schlüssel ■ <i>DES3 168</i>: Triple DES mit 168-Bit-Schlüssel ■ <i>none</i>: keine Verschlüsselung <p>Diese Werte sind nur verfügbar, wenn unter Encapsulation <i>PPP</i>, <i>Async PPP over X.75</i>, <i>Async PPP over X.75/T.70/BTX</i> oder <i>X.25_PPP</i> 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 6-10: **WAN PARTNER** ➤ **ADD**

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

Protokolle		Encapsulierung	Komprimierung
IP	IPX		STAC, MS-STAC
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 6-11: Encapsulierung und Komprimierung

ToDo Machen Sie folgende Eintragungen:

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

Rufnummern eintragen

X1000 Setup Tool	BinTec Communications AG				
[WAN][ADD][WAN Numbers]: WAN Numbers (BigBoss)	MyX1000				
<p>WAN Numbers for this partner:</p> <table border="1"> <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> to edit					

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

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

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

Ein weiteres Menüfenster erscheint:

X1000 Setup Tool	BinTec Communications AG						
[WAN][ADD][WAN NUMBERS][ADD]:Add or Change WAN Numb.(BigBoss)	MyX1000						
<table border="1"> <tbody> <tr> <td>Number</td> <td>0911987654321</td> </tr> <tr> <td>Direction</td> <td>outgoing</td> </tr> <tr> <td colspan="2">Advanced Settings ></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 6-12: **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 X1000 einwählen soll.

Tabelle 6-13: **Direction**



Wenn **X1000** 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	X1000 akzeptiert eingehende Rufe z. B. mit:	Ausgehende Rufe, d. h. X1000 baut eine Verbindung zum WAN-Partner auf mit:
*	Entspricht einer Gruppe von keiner bis mehreren Ziffern.	Wird ignoriert.	123*	123, 1234, 123789	123
?	Entspricht genau einer Ziffer.	Wird durch 0 ersetzt.	123?	1234, 1238, 1231	1230
[a-b]	Definiert einen Bereich von passenden Ziffern.	Die erste Ziffer des definierten Bereiches wird verwendet.	123[5-9]	1235, 1237, 1239	1235
[^a-b]	Definiert einen Bereich von verbotenen Ziffern.	Die erste Ziffer nach dem definierten Bereich wird verwendet.	123[^0-5]	1236, 1238, 1239	1236
{ab}	Entspricht einer Gruppe von optionalen Ziffern.	Wird verwendet.	{00}1234	001234 und 1234	001234

Tabelle 6-14: 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 **X1000** den Anrufer identifizieren (➤➤ **CLID**), wenn dieser als WAN-Partner eingetragen ist. Nach der Identifizierung mit CLID kann der Router zusätzlich eine PPP-Authentisierung mit dem WAN-Partner durchführen, bevor der Ruf angenommen wird. Dazu benötigt der Router Vergleichsdaten, die Sie hier eintragen. Zunächst legen Sie fest, welche Authentisierungsverhandlung ausgeführt werden soll, anschließend tragen Sie ein gemeinsames Paßwort und zwei Kennungen ein. Diese Daten erhalten Sie z. B. von Ihrem Internet Service Provider oder dem Systemadministrator der Firmenzentrale. Nur wenn diese Daten, die Sie auf **X1000** hier eintragen, mit den Daten des Anrufers übereinstimmen, wird der Ruf angenommen.

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

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

X1000 Setup Tool		BinTec Communications AG
[WAN][ADD][PPP]: PPP Settings (BigBoss)		MyX1000
Authentication	CHAP + PAP	
Partner PPP ID	BigBoss	
Local PPP ID	LittleIndian	
PPP Password	Secret	
Keepalives	off	
Link Quality Monitoring	off	
OK		CANCEL
Use <Space> to select		

Das Menü enthält folgende Felder:

Feld	Bedeutung
Authentication	Authentisierungsprotokoll.
Partner PPP ID	Kennung des WAN-Partners.
Local PPP ID	X1000s Kennung.
PPP Password	Paßwort.
Keepalives	Aktiviert Keepalive-Pakete.
Link Quality Monitoring	PPP Link Quality Monitoring nach RFC 1989.

Tabelle 6-15: **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>none</i>	Kein PPP-Authentisierungsprotokoll ausführen.

Tabelle 6-16: **Authentication**

ToDo Machen Sie folgende Eintragungen:

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



Die Vorgehensweise bei der Eingabe von Paßwörtern ist unter "[Paßwortänderung](#)", Seite 128 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 **X1000** nicht, welches Authentisierungsprotokoll mit diesem WAN-Partner festgelegt ist. Damit der Ruf trotzdem angenommen werden kann, greift **X1000** auf allgemeine Einstellungen im PPP zurück, die Sie nach Bedarf verändern können (siehe [Kapitel 7.1.3, Seite 220](#)).

Shorthold festlegen

Stellen Sie als nächstes Shorthold ein, um Gebühren zu sparen. **X1000** bricht dann die ISDN-Verbindung ab, wenn keine Daten mehr fließen. Mit statischem bzw. dynamischem Shorthold legen Sie fest, nach welchem Inaktivitätsintervall (Idle Timer) **X1000** 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 (AOCD). Fragen Sie Ihre Telefongesellschaft!



Es ist unbedingt notwendig, bei Nutzung des dynamischen Shortholds zusätzlich einen statischen Shorthold einzustellen, um beim Ausfall von AOCD (advice of charge during the call, Übermittlung der Gebührenintervalle während der Verbindung) keine Dauerwahlverbindung zu haben.

Dabei sollten Sie sicherstellen, daß der statische Shorthold später einsetzt als der dynamische. Andernfalls beendet **X1000** die Verbindung immer gemäß dem statischen Shorthold, der dynamische Shorthold kann nicht greifen. Geben Sie deshalb in diesem Fall als **Static Short Hold (sec)** einen Wert ein, der etwas über dem maximal zu erwartenden dynamischen Inaktivitätsintervall liegt.

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

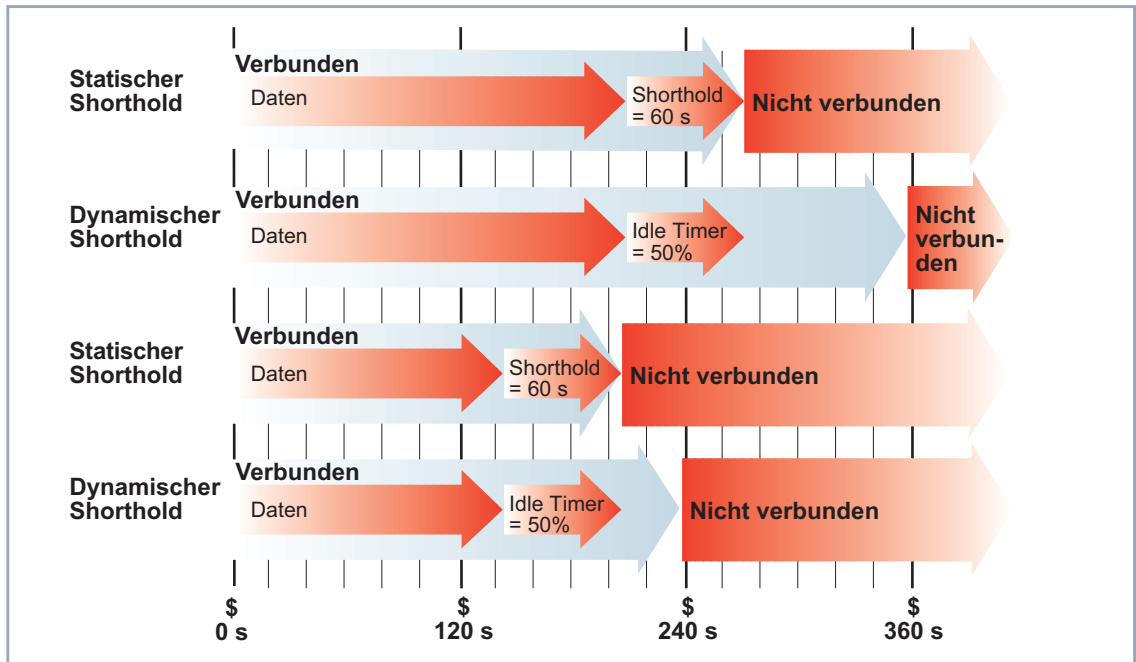


Bild 6-5: Dynamischer und statischer Shorthold

Gehen Sie folgendermaßen vor:

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

X1000 Setup Tool	BinTec Communications AG
[WAN][ADD][ADVANCED]: Advanced Settings (BigBoss)	MyX1000
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 Prozent für dynamischen Shorthold. Nur wirksam, wenn Gebühreninformationen während der Verbindung übermittelt werden (AOCD).

Tabelle 6-17: **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 sich 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**.

X1000 Setup Tool		BinTec Communications AG
[WAN][ADD][IP]: IP Configuration (BigBoss)		MyX1000
IP Transit Network		no
local IP Address		
Partner's LAN IP Address		10.1.1.0
Partner's LAN Netmask		255.255.255.0
Advanced Settings >		
	SAVE	CANCEL
Use <Space> to select		

Das Menü enthält folgende Felder:

Feld	Bedeutung
IP Transit Network	Legt fest, ob X1000 ein Transit Network zum WAN-Partner nutzt.
local IP Address	IP-Adresse von X1000 . Im Normalfall müssen Sie hier keinen Eintrag machen, außer Sie richten für einen Ihrer WAN-Partner ein Transitnetzwerk ein (siehe Kapitel 7.2.6, Seite 249).
local ISDN IP Address	ISDN-IP-Adresse von X1000 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 Ihres WAN-Partners.
Partner's LAN Netmask	Netzmaske des LAN Ihres WAN-Partners. Wenn Sie keinen Eintrag machen, trägt X1000 eine Standardnetzmaske für die unter Partner's LAN IP Address verwendete Netzklasse ein.

Tabelle 6-18: **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 Internet-Zugang einrichten, kennen Sie normalerweise die IP-Adresse Ihres Internet Service Providers (ISP) nicht und **X1000** 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: X1000s** 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 **X1000s** statische IP-Adresse, die Sie vom ISP erhalten.
 - Keine Eintragungen für **Partner's LAN IP Address** und **Partner's LAN Netmask**.

Wenn Sie mehr wissen wollen, z. B. was ein Transit Network eigentlich ist und wofür Sie es brauchen, siehe [Kapitel 7.2.6, Seite 249](#).



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 **X1000** eingetragen. Für jeden WAN-Partner wird automatisch ein Routing-Eintrag in der Routing-Tabelle von **X1000** 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**:

X1000 Setup Tool	BinTec Communications AG					
[IP][ROUTING]: IP Routing	MyX1000					
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 **X1000** 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 diesem Fall [Kapitel 8.2.12, Seite 357](#).

X1000 Setup Tool	BinTec Communications AG
[IP][ROUTING][ADD]: IP Routing	MyX1000
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).
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 X1000 die IP-Pakete weitergeben soll.
Metric	Je niedriger der Wert, desto höhere Priorität besitzt die Route (Wertebereich 1...14).

Tabelle 6-19: **IP** ➤ **ROUTING** ➤ **ADD**

Das Feld **Network** enthält folgende Auswahlmöglichkeiten:

Mögliche Werte	Bedeutung
<i>LAN</i>	Route zu einem Ziel-Host oder -LAN, das über X1000s 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>	X1000 verwirft Datenpakete, die diese Route benutzen, und übermittelt dem Absender eine Meldung, daß das Ziel des Paketes unerreichbar ist.
<i>Ignore</i>	X1000 verwirft Datenpakete, die diese Route benutzen, ohne eine Statusmeldung zu senden.

Tabelle 6-20: **Network**



Sie können auf **X1000** nur eine einzige Default-Route eintragen: Wenn Sie also einen Zugang zum Internet einrichten, dann tragen Sie die Route zu Ihrem Internet Service Provider (ISP) als Default-Route ein.

Wenn Sie eine Firmennetzanbindung machen, dann tragen Sie die Route zur Zentrale nur dann als Default-Route ein, wenn Sie keinen Internet-Zugang über **X1000** einrichten.

Wenn Sie sowohl einen Zugang zum Internet, als auch eine Firmennetzanbindung einrichten, dann tragen Sie zum ISP eine Default-Route und zur Firmenzentrale eine Netzwerkroute ein.

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

- Wählen Sie **Route Type** aus: *Default Route*.
- Wählen Sie **Network** aus: *WAN without transit network*.
- Wählen Sie **Partner / Interface** aus: z. B. *GoInternet*.

➤ Geben Sie **Metric** ein, z. B. **1**.

➤ Bestätigen Sie mit **SAVE**.

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



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

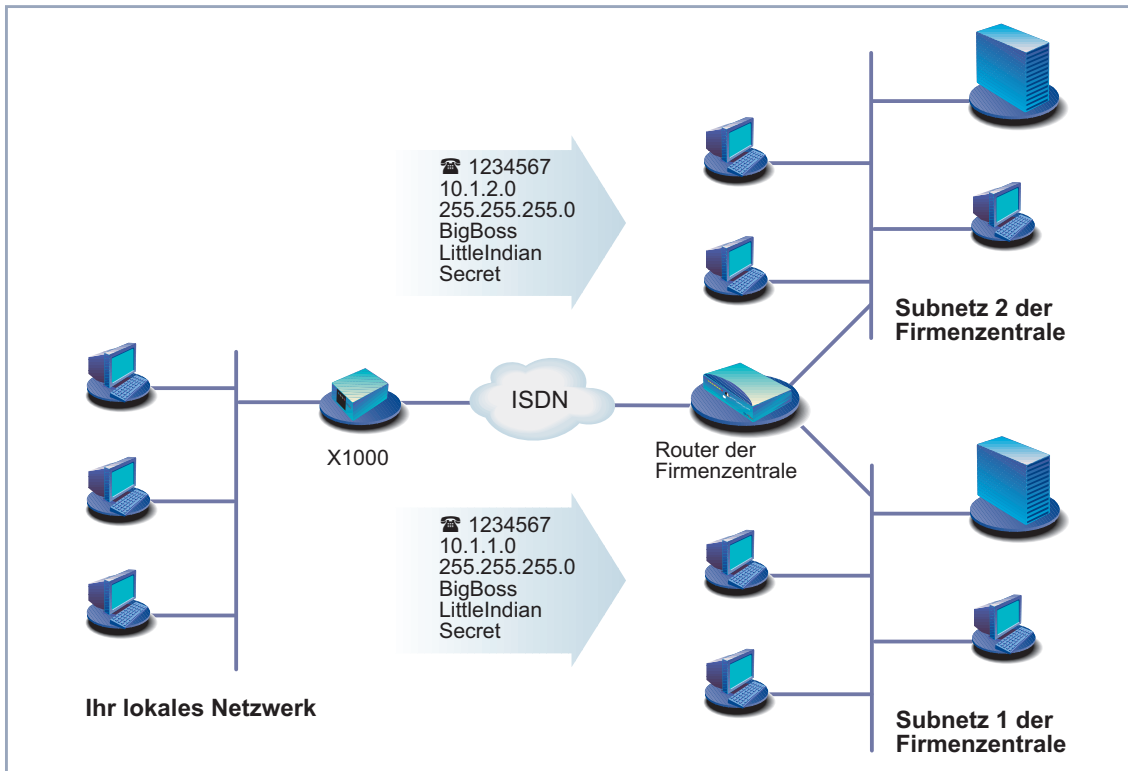


Bild 6-6: Firmennetzzentrale mit mehreren angeschlossenen LANs

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

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

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

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

Network Address Translation (NAT) aktivieren

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

Detaillierte Informationen zu Network Address Translation (NAT) finden Sie in [Kapitel 8.2.7, Seite 333](#).

Gehen Sie folgendermaßen vor, um NAT zu aktivieren:

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

```

X1000 Setup Tool                               BinTec Communications AG
[IP][NAT]: NAT Configuration                     MyX1000

Select IP Interface to be configured for NAT

Name          Nat      static mappings
GoInternet    off
BigBoss       off
enl           off
enl-snap      off

EXIT

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

```

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

```

X1000 Setup Tool                               BinTec Communications AG
[IP][NAT][CONFIG]: NAT Configuration (GoInternet) MyX1000

Network Address Translation      on

Configuration for sessions requested from outside

Service      Destination      Source Dep.      Dest. Dep.      Port Remap

ADD          DELETE          SAVE          CANCEL

Use <Space> to select

```

ToDo Machen Sie folgende Eintragungen:

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

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

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

6.2.2 Mit X1000 ins Internet

Beispiele Im Anschluß an die in [Kapitel 6.2.1, Seite 169](#) beschriebene allgemeine Vorgehensweise, nach der Sie prinzipiell für jeden Internet Service Provider (ISP) vorgehen können, sind hier einige Beispiele angegeben. Sie zeigen, wie Sie Ihren Internet-Zugang mit bestimmten Providern schnell und einfach einrichten.

- Beispiel 1: T-Online

- Beispiel 2: Compuserve

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

Los geht's:

Beispiel 1: T-Online

Wenn Sie einen Internet-Zugang über den Provider T-Online herstellen wollen, gehen Sie folgendermaßen vor:

WAN-Partner einrichten

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

Rufnummer eintragen

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

- Bestätigen Sie mit **SAVE**.
Die Rufnummer, mit der Sie sich bei T-Online einwählen, steht nun in der Liste.

- Verlassen Sie **WAN PARTNER** ➤ **ADD** ➤ **WAN NUMBERS** mit **EXIT**.

PPP-Authentisierung festlegen

- Wählen Sie **PPP** aus und bestätigen Sie mit der **Eingabetaste**.
- Wählen Sie **Authentication** aus: *CHAP + PAP*.
- Geben Sie **Partner PPP ID** (=Providername) ein: *T_Online*.
- Geben Sie **Local PPP ID** (= Ihr Benutzername) ein:
z. B. *000460004256091169386#0001*.



Der T-Online Benutzername setzt sich folgendermaßen zusammen:
<Anschlußkennung><T-Online-Nummer>#<Mitbenutzernummer>
Die Anschlußkennung ist 12-stellig, hier: *000460004256*.
Die T-Online-Nummer ist die Rufnummer, hier: *091169386*.
Die Mitbenutzernummer ist 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** (=Paßwort) ein.
- Deaktivieren Sie **Keepalives**: *off*.
- Deaktivieren Sie **Link Quality Monitoring**: *off*.
- Bestätigen Sie mit **OK**.

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

Shorthold festlegen

- Wählen Sie **Advanced Settings** aus und bestätigen Sie mit der **Eingabetaste**.
- Wählen Sie **Callback** aus: *no*.
- Geben Sie **Static Short Hold (sec)** ein, mindestens: *60*.
- Geben Sie **Idle for Dynamic Short Hold (%)** ein, z. B. *0*.
- Geben Sie **Delay after Connection Failure (sec)** ein, z. B. *300*.
- Überspringen Sie **Extended Interface Settings (optional)**.
- Wählen Sie **Channel Bundling** aus: *no*.
- Wählen Sie **Layer 1 Protocol** aus: *ISDN 64 kbps*.

- Bestätigen Sie mit **OK**.
Sie befinden sich wieder im Menü **WAN PARTNER** ➤ **ADD**.
- IP-Konfiguration durchführen**
 - Wählen Sie **IP** aus und bestätigen Sie mit der **Eingabetaste**.
 - Wählen Sie **IP Transit Network** aus: *dynamic client*.
 - Wählen Sie **Advanced Settings** aus und bestätigen Sie mit der **Eingabetaste**.
 - Wählen sie **RIP Send**: *none*.
 - Wählen Sie **RIP Receive**: *none*.
 - Aktivieren Sie **Van Jacobson Header Compression**: *on*.
 - Wählen Sie **Dynamic Name Server Negotiation** aus: *client (receive)*.
 - Deaktivieren Sie **IP Accounting**: *off*.
 - Deaktivieren Sie **Back Route Verify**: *off*.
 - Wählen Sie **Route Announce** aus: *up or dormant*.
 - Wählen Sie **Proxy Arp** aus: *off*.
 - Bestätigen Sie mit **OK**.
 - Bestätigen Sie mit **SAVE**.
 - Bestätigen Sie erneut mit **SAVE**.
 - Verlassen Sie **WAN PARTNER** mit **EXIT**.
- Routing-Eintrag erstellen**
 - Gehen Sie zu **IP** ➤ **ROUTING**.
 - Fügen Sie einen neuen Eintrag mit **ADD** hinzu.
 - Wählen Sie **Route Type** aus: *Default route*.
 - Wählen Sie **Network** aus: *WAN without transit network*.
 - Wählen Sie **Partner / Interface** aus: *T_Online*.
 - Geben Sie **Metric** ein, z. B. *1*.
 - Bestätigen Sie mit **SAVE**.
 - Verlassen Sie **IP** ➤ **ROUTING** mit **EXIT**.
- NAT aktivieren**
 - Gehen Sie zu **IP** ➤ **NETWORK ADDRESS TRANSLATION**.

- Wählen Sie das IP Interface T_Online aus und bestätigen Sie mit der **Eingabetaste**.
- Wählen Sie **Network Address Translation** aus: *on*.
- Bestätigen Sie mit **SAVE**.
- Verlassen Sie **IP** ➤ **NETWORK ADDRESS TRANSLATION** mit **EXIT**.
- Verlassen Sie **IP** mit **EXIT**.
Sie befinden sich wieder im Hauptmenü.
Die Konfiguration des Internet-Zugangs über T-Online ist abgeschlossen.

Beispiel 2: Compuserve

Wenn Sie Ihren Internet-Zugang über den Provider Compuserve herstellen wollen, gehen Sie folgendermaßen vor:



Hier wird der Zugang zu Compuserve über direkte Einwahl auf einen Compuserve Netzwerkknoten beschrieben.

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

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

WAN-Partner einrichten

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

Rufnummer eintragen

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

- Bestätigen Sie mit **SAVE**.
Die Rufnummer, mit der Sie sich bei CompuServe einwählen, steht nun in der Liste.
- Verlassen Sie **WAN PARTNER** ➤ **ADD** ➤ **WAN NUMBERS** mit **EXIT**.
- PPP-Authentisierung festlegen**
 - Wählen Sie **PPP** aus und bestätigen Sie mit der **Eingabetaste**.
 - Wählen Sie **Authentication** aus: *none*.
 - Deaktivieren Sie **Keepalives**: *off*.
 - Deaktivieren Sie **Link Quality Monitoring**: *off*.
 - Bestätigen Sie mit **OK**.
Sie befinden sich wieder im Menü **WAN PARTNER** ➤ **ADD**.
- Shorthold festlegen**
 - Wählen Sie **Advanced Settings** aus und bestätigen Sie mit der **Eingabetaste**.
 - Wählen Sie **Callback** aus: *no*.
 - Geben Sie **Static Short Hold (sec)** ein: *120*. (Der hier eingegebene Wert muß größer oder gleich 120 sein).
 - Geben Sie **Idle for Dynamic Short Hold (%)** ein, z. B. *0*.
 - Geben Sie **Delay after Connection Failure (sec)** ein, z. B. *300*.
 - Überspringen Sie **Extended Interface Settings (optional)**.
 - Wählen Sie **Channel Bundling** aus: *no*.
 - Wählen Sie **Layer 1 Protocol** aus: *ISDN 64 kbps*.
- Authentisierung festlegen**
 - Wählen Sie **Provider Configuration** aus und bestätigen Sie mit der **Eingabetaste**.
 - Wählen Sie **Provider** aus: *CompuServe Network*.
 - Geben Sie **Host** ein: *CIS*.
 - Geben Sie **User ID** (= Ihr Benutzername) ein.
 - Geben Sie **Password** (=Paßwort) ein.
 - Bestätigen Sie mit **OK**.

- Bestätigen Sie erneut mit **OK**.
Sie befinden sich wieder im Menü **WAN PARTNER** ➤ **ADD**.
- IP-Konfiguration durchführen**
 - Wählen Sie **IP** aus und bestätigen Sie mit der **Eingabetaste**.
 - Wählen Sie **IP Transit Network** aus: *dynamic client*.
 - Wählen Sie **Advanced Settings** aus und bestätigen Sie mit der **Eingabetaste**.
 - Wählen sie **RIP Send**: *none*.
 - Wählen Sie **RIP Receive**: *none*.
 - Deaktivieren Sie **Van Jacobson Header Compression**: *off*.
 - Wählen Sie **Dynamic Name Server Negotiation** aus: *client (receive)*.
 - Deaktivieren Sie **IP Accounting**: *off*.
 - Deaktivieren Sie **Back Route Verify**: *off*.
 - Wählen Sie **Route Announce** aus: *up or dormant*.
 - Wählen Sie **Proxy Arp** aus: *off*.
 - Bestätigen Sie mit **OK**.
 - Bestätigen Sie mit **SAVE**.
 - Bestätigen Sie erneut mit **SAVE**.
 - Verlassen Sie **WAN PARTNER** mit **EXIT**.
- Routing-Eintrag erstellen**
 - Gehen Sie zu **IP** ➤ **ROUTING**.
 - Fügen Sie einen neuen Eintrag mit **ADD** hinzu.
 - Wählen Sie **Route Type** aus: *Default route*.
 - Wählen Sie **Network** aus: *WAN without transit network*.
 - Wählen Sie **Partner / Interface** aus: *COMPUSERVE*.
 - Geben Sie **Metric** ein, z. B. *1*.
 - Bestätigen Sie mit **SAVE**.
 - Verlassen Sie **IP** ➤ **ROUTING** mit **EXIT**.
- NAT aktivieren**
 - Gehen zu **IP** ➤ **NETWORK ADDRESS TRANSLATION**.

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

Sie befinden sich wieder im Hauptmenü.

Die Konfiguration des Internet-Zugangs über Compuserve ist abgeschlossen.

6.2.3 Ins Firmennetz einwählen

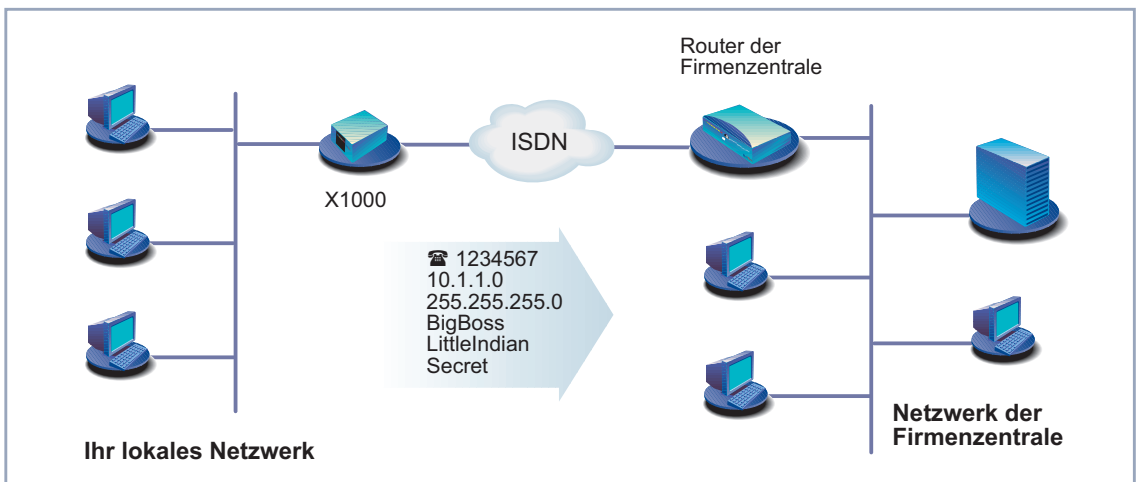


Bild 6-7: **X1000** und Ihre Firmenzentrale

Im ersten Teil dieses Kapitels ist eine schnelle Konfiguration für eine Firmennetzanbindung (LAN-LAN-Kopplung) mit **X1000** Schritt für Schritt dargestellt. Im zweiten Teil erklären wir Ihnen, wie Sie vorgehen müssen, wenn sich ein Außendienstmitarbeiter oder ein Mitarbeiter vom Heimarbeitsplatz aus in die Firmenzentrale einwählen will.

Firmennetzanbindung: Allgemeines Beispiel

Legen Sie sich die Daten zurecht, die Sie vom Systemadministrator der Firmenzentrale erhalten haben (siehe auch [Kapitel 3.2.1, Seite 40](#)). Wenn Sie sich an manchen Stellen nicht sicher sind, beachten Sie [Kapitel 6.2.1, Seite 169](#).

Gehen Sie folgendermaßen vor:

- WAN-Partner einrichten**
- Gehen Sie zu **WAN PARTNER** ➤ **ADD**.
 - Geben Sie **Partner Name** (= Kennung der Firmenzentrale) ein, z. B. *BigBoss*.
 - Wählen Sie **Encapsulation** aus: *PPP*.
 - Wählen Sie **Compression** aus: *STAC*.
 - Wählen Sie **Encryption** aus: *none*.
- Rufnummer eintragen**
- Wählen Sie **WAN Numbers** aus und bestätigen Sie mit der **Eingabetaste**.
 - Fügen Sie einen neuen Eintrag mit **ADD** hinzu.
 - Geben Sie **Number** (= Rufnummer des Routers der Firmenzentrale) ein, z. B. *0911987654321*.
 - Wählen Sie **Direction** aus: *outgoing*.
 - Bestätigen Sie mit **SAVE**.
- Die Rufnummer, mit der Sie sich bei der Firmenzentrale einwählen, steht nun in der Liste.
- Verlassen Sie **WAN PARTNER** ➤ **ADD** ➤ **WAN NUMBERS** mit **EXIT**.
- PPP-Authentisierung festlegen**
- Wählen Sie **PPP** aus und bestätigen Sie mit der **Eingabetaste**.
 - Wählen Sie **Authentication** aus: *CHAP + PAP*.
 - Geben Sie **Partner PPP ID** (=Kennung der Firmenzentrale) ein, z. B. *BigBoss*.
 - Geben Sie **Local PPP ID** (=Ihre eigene Kennung) ein, z. B. *LittleIndian*.
 - Geben Sie **PPP Password** (=Gemeinsames Paßwort für diese Verbindung) ein.
 - Deaktivieren Sie **Keepalives**: *off*.
 - Deaktivieren Sie **Link Quality Monitoring**: *off*.

- Bestätigen Sie mit **OK**.
Sie befinden sich wieder im Menü **WAN PARTNER** ➤ **ADD**.
- Shorthold festlegen** ➤ Wählen Sie **Advanced Settings** aus und bestätigen Sie mit der **Eingabetaste**.
 - Wählen Sie **Callback** aus: *no*.
 - Geben Sie **Static Short Hold (sec)** ein, z. B. *20*.
 - Geben Sie **Idle for Dynamic Short Hold (%)** ein, z. B. *0*.
 - Geben Sie **Delay after Connection Failure (sec)** ein, z. B. *300*.
 - Überspringen Sie **Extended Interface Settings (optional)**.
 - Wählen Sie **Channel Bundling** aus: *no*.
 - Wählen Sie **Layer 1 Protocol** aus: *ISDN 64 kbps*.
 - Bestätigen Sie mit **OK**.
Sie befinden sich wieder im Menü **WAN PARTNER** ➤ **ADD**.
- IP-Konfiguration durchführen** ➤ Wählen Sie **IP** aus und bestätigen Sie mit der **Eingabetaste**.
 - Wählen Sie **IP Transit Network** aus: *no*.
 - Geben Sie **Partner's LAN IP Address** (= Netzadresse der Firmenzentrale) ein: z. B. *10.1.1.0*.
 - Geben Sie **Partner's LAN Netmask** (= Netzmaske der Firmenzentrale) ein, z. B. *255.255.255.0*.
 - Wählen Sie **Advanced Settings** aus und bestätigen Sie mit der **Eingabetaste**.
 - Wählen sie **RIP Send**: *none*.
 - Wählen Sie **RIP Receive**: *none*.
 - Aktivieren Sie **Van Jacobson Header Compression**: *off*.
 - Wählen Sie **Dynamic Name Server Negotiation** aus: *yes* (wenn Sie Internet-Zugang konfiguriert haben) oder *off* (wenn Sie keinen Internet-Zugang konfiguriert haben).
 - Aktivieren Sie **IP Accounting**: *on*.
 - Aktivieren Sie **Back Route Verify**: *on*.

- Wählen Sie **Route Announce** aus: *up or dormant*.
- Wählen Sie **Proxy Arp** aus: *off*.
- Bestätigen Sie mit **OK**.
- Bestätigen Sie mit **SAVE**.
- Bestätigen Sie erneut mit **SAVE**.
- Verlassen Sie **WAN PARTNER** mit **EXIT**.

Sie befinden sich wieder im Hauptmenü.

Die Konfiguration des Zugangs zur Firmennetzzentrale ist abgeschlossen.

Routing-Eintrag erstellen



Wenn Sie keinen Internet-Zugang eingerichtet haben, dann können Sie für den Zugang zur Firmenzentrale eine Default-Route einrichten (siehe [Kapitel 6.2.1, Seite 169](#)):

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



Wenn das Netzwerk der Firmenzentrale aus mehreren LANs (Subnetzen) besteht und Sie keine Default-Route zur Firmenzentrale einrichten, dann müssen Sie für jedes LAN, das Sie erreichen wollen, einen eigenen Routing-Eintrag erstellen. Beachten Sie dazu die Hinweise in [Kapitel 6.2.1, Seite 169](#) und [Bild 6-6, Seite 192](#).

- Wiederholen Sie die Schritte für das Erstellen eines Routing-Eintrags so oft, bis Sie alle notwendigen Routen eingetragen haben.
- Bestätigen Sie mit **SAVE**.
- Verlassen Sie **IP** ➤ **ROUTING** mit **EXIT**.
- Verlassen Sie **IP** mit **EXIT**.

Firmennetzanbindung: Dial-in (ohne Router)

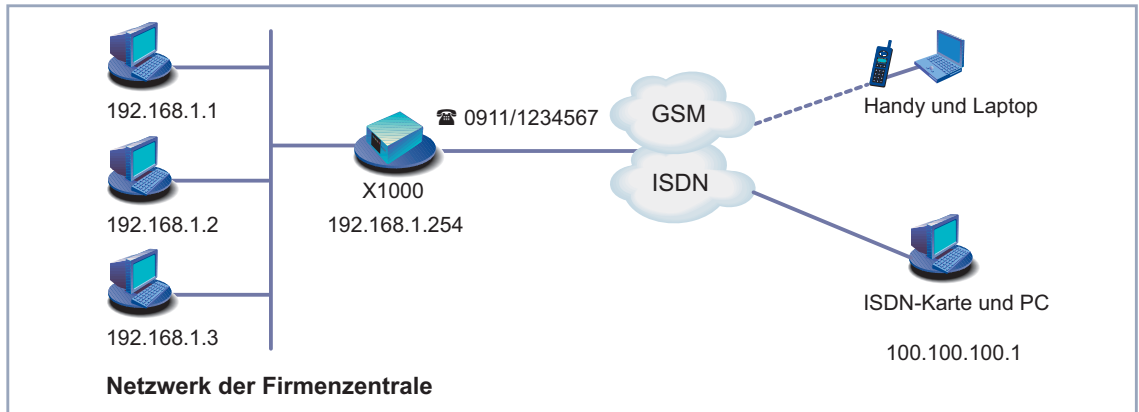


Bild 6-8: Szenario für Dial-in

Um auf die Daten seiner Firmenzentrale zuzugreifen, kann sich ein Außendienstmitarbeiter über Laptop und Handy im Netz der Zentrale einwählen, ein Mitarbeiter am Heimarbeitsplatz braucht entweder eine ISDN-Karte in seinem PC oder ein Modem, wenn er keinen Router hat. Prinzipiell ist die Konfiguration von **X1000** und auf dem PC bzw. Laptop in allen diesen Fällen identisch. Außendienstmitarbeiter, die ein Handy der Marke Nokia Communicator verwenden, müssen noch zusätzliche Einstellungen vornehmen, die am Ende des folgenden Abschnitts beschrieben sind.

Die Konfiguration erfolgt in zwei bzw. drei Schritten.

- Konfiguration von **X1000**
- Konfiguration des PC
- Konfiguration für Windows-Netzwerk (optional)

Konfiguration X1000 Nach der Grundkonfiguration von **X1000** (siehe [Kapitel 3.5.1, Seite 58](#) und [Kapitel 6.1, Seite 137](#)) legen Sie den gewünschten Dial-in-Partner als WAN Partner an.

- WAN-Partner einrichten**
- Gehen Sie zu **WAN PARTNER** ➤ **ADD**.
 - Geben Sie **Partner Name** ein, z. B. *Client Dialin*.

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

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

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

PPP-Authentisierung festlegen

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

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

➤ Geben Sie **Partner PPP ID** ein, z. B. *clientdialin*.

➤ Lassen Sie **Local PPP ID** (= Ihre eigene Kennung) leer (bei ausschließlichem Dial-in).

➤ Geben Sie **PPP Password** (= Gemeinsames Paßwort für diese Verbindung) ein.

➤ Deaktivieren Sie **Keepalives**: *off*.

➤ Deaktivieren Sie **Link Quality Monitoring**: *off*.

➤ Bestätigen Sie mit **OK**.

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

IP-Konfiguration durchführen

Definieren Sie die Route zu Ihrem Dial-in-Partner:

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

➤ Wählen Sie **IP Transit Network** aus: *Dynamic server*.

Adreß-Pool festlegen

➤ Wählen Sie **Advanced Settings** aus und bestätigen Sie mit der **Eingabetaste**.

➤ Wählen Sie **RIP Send**: *none*.

➤ Wählen Sie **RIP Receive**: *none*.

➤ Deaktivieren Sie **Van Jacobson Header Compression**: *off*.

➤ Deaktivieren Sie **Dynamic Name Server Negotiation**: *off*.

➤ Geben Sie **IP Address Pool** ein: *1*.

➤ Deaktivieren Sie **IP Accounting**: *off*.

➤ Deaktivieren Sie **Back Route Verify**: *off*.

➤ Wählen Sie **Route Announce** aus: *up or dormant*.

➤ Wählen Sie **Proxy Arp** aus: *off*.

- Bestätigen Sie mit **OK**.
 - Bestätigen Sie mit **SAVE**.
Sie befinden sich wieder im Menü **WAN PARTNER** ➤ **ADD**.
- Shorthand festlegen**
- Wählen Sie **Advanced Settings** aus und bestätigen Sie mit der **Eingabetaste**.
 - Wählen Sie **Callback** aus: *no*.
 - Geben Sie **Static Short Hold (sec)** ein, z. B. *300*, d.h. einen hohen Wert.
 - Geben Sie **Idle for Dynamic Short Hold (%)** ein, z. B. *0*.
 - Geben Sie **Delay after Connection Failure (sec)** ein, z. B. *30*.
 - Überspringen Sie **Extended Interface Settings (optional)**.
 - Wählen Sie **Channel Bundling** aus: *no*.
 - Wählen Sie **Layer 1 Protocol** aus: *ISDN 64 kbps*.
 - Bestätigen Sie mit **OK**.
Sie befinden sich wieder im Menü **WAN PARTNER** ➤ **ADD**.
 - Bestätigen Sie mit **Save**.
 - Verlassen Sie **WAN PARTNER** mit **EXIT**.
- IP-Adresse eintragen**
- Gehen Sie zu **IP** ➤ **IP ADDRESS POOL WAN (PPP)** ➤ **ADD**.
 - Geben Sie **Pool ID** ein, z. B. *1*.
 - Geben Sie **IP Address** (= IP-Adresse Ihres Dial-in-Partners) ein, z. B. *100.100.100.1*.
 - Geben Sie **Number of consecutive addresses** ein, z. B. *1*.
 - Bestätigen Sie mit **SAVE**.
 - Verlassen Sie **IP** ➤ **IP ADDRESS POOL WAN (PPP)** mit **EXIT**.
 - Verlassen Sie **IP** mit **EXIT**.
- Rufnummer eintragen**
- Gehen Sie zu **CM-1BRI, ISDN S0** ➤ **INCOMING CALL ANSWERING** ➤ **ADD**.
 - Wählen Sie **Item** aus: *PPP (routing)*.
Mit der Einstellung *PPP (routing)* wird das benutzte Protokoll (z.B. ISDN 64 kbps oder V110 (9600)) automatisch erkannt.

- Geben Sie **Number** ein, z. B. 1234567 (= Telefonnummer, über die sich der Dial-in-Partner einwählen soll).



Tragen Sie unter **Number** nur Ihre Rufnummer ohne Vorwahl ein. Beim Anschluß von **X1000** an eine TK-Anlage, dürfen Sie nur die Nebenstellenummer eingeben, die bei **X1000** ankommt. (Beachten Sie dazu auch den Hinweis in [Kapitel 6.1.4, Seite 146](#)).

- Wählen Sie **Mode** aus: *right to left*.
- **Username** können Sie frei lassen.
- Wählen Sie **Bearer** aus: *any*.
- Bestätigen Sie mit **SAVE**.
- Verlassen Sie **ICM-1BRI**, **ISDN S0** ➤ **INCOMING CALL ANSWERING** mit **EXIT**.
- Bestätigen Sie mit **SAVE**.

Nokia Communicator

Wenn Sie ein Handy der Marke Nokia Communicator verwenden, müssen Sie zusätzlich folgende Einträge vornehmen, damit das Handy eine Verbindung zum Firmennetz aufbauen kann:

- Gehen Sie zu **PPP**.
- Aktivieren Sie **PPP Link Quality Monitoring**: *yes*.
- Gehen Sie zu **WAN PARTNER** ➤ **ADD** ➤ **PPP**.
- Aktivieren Sie **Link Quality Monitoring**: *on*.

Konfiguration des PC unter Windows NT

Im folgenden finden Sie die Schritte, die bei der Konfiguration des PCs bzw. Laptops mit dem Betriebssystem Windows NT notwendig sind. Unter Windows 95 bzw. 98 müssen Sie im Prinzip dieselben Punkte beachten, sodaß Sie anhand der Liste die Konfiguration ebenfalls erfolgreich durchführen werden.

Folgende Schritte sind erforderlich:

- Installieren der ISDN/GSM-Karte bzw. des Modems zusammen mit dem entsprechenden DFÜ-Treiber. (Beachten Sie die Dokumentation Ihrer Karte bzw. Ihres Modems und folgen Sie den Anweisungen auf dem Bildschirm.)

- Überprüfen, ob das TCP/IP-Protokoll installiert ist (im Windows Startmenü unter **Einstellungen ▶ Systemsteuerung ▶ Netzwerk**) bzw. Installieren diese Protokolls (siehe [Kapitel 3.2.2, Seite 43](#)).
- Installierte Karte kontrollieren (im Register **Netzwerkkarte**).
- Überprüfen, ob RAS-Dienst installiert ist bzw. RAS-Dienst installieren (im Register **Dienste**).
- Verlassen des Menüs **Netzwerk** mit **OK**. Das TCP/IP-Protokoll wird auf den Dial-up-Adapter gebunden. Wenn die Installation erfolgreich abgeschlossen ist, sind die virtuellen Modems aufgelistet (**Einstellungen ▶ Systemsteuerung ▶ Modems**).
- Neuen Telefonbucheintrag für die Verbindung vornehmen (**Programme ▶ Zubehör ▶ DFÜ-Netzwerk**). U.a. muß die Telefonnummer eingetragen werden, unter der **X1000** Routing-Anrufe entgegennimmt.
- Überprüfen des Telefonbucheintrags (**Weiteres ▶ Eintrags- und Modemeigenschaften bearbeiten** im Register **Einträge**).
- Im Register **Server** darf nur **TCP/IP** als Netzwerkprotokoll ausgewählt sein.
- Verbindung erstellen (**Wählen**).
- Eintragen von Benutzername und Kennwort (= **Partner PPP ID** und **PPP Password** unter **WAN PARTNER ▶ ADD ▶ PPP** auf **X1000**).
- Nach Verlassen des Menüs mit **OK** wird die Verbindung hergestellt.



Wenn Sie sich in ein Windows-Netzwerk einwählen möchten, müssen Sie noch einige zusätzliche Konfigurationsschritte vornehmen.

Konfiguration für Windows-Netzwerk

Wenn Sie sich an einem Windows-NT-Server anmelden möchten, müssen Sie bzw. der Netzwerk-Administrator an zwei Stellen konfigurieren:

- auf dem Windows NT Domain Server
- auf dem Windows-Rechner

Windows-NT-Server Auf dem Windows-NT-Server muß der Administrator folgende Konfigurationsschritte durchführen:

- einen Benutzer im Benutzermanager anlegen
- den Dial-in-PC als Mitglied der Domäne anlegen
- Namensauflösung sollte durchgeführt werden (WINS Server, DNS Server oder LMHOSTS-Datei).

Windows Client Auf dem Windows-PC müssen folgende Konfigurationsschritte durchgeführt werden:

- Eintragen des NetBIOS-Namens des Rechners und des Gruppennamens (d.h. im Windows Startmenü unter **Einstellungen** ▶ **Systemsteuerung** ▶ **Netzwerk** müssen im Register **Identifikation** der Gruppenname und der Name der NT-Domäne identisch sein).
- Client für Microsoft-Netzwerke installieren und dort die Domäne des Servers (z. B. **BINTECDOM**) eintragen.

6.3 Konfigurationsdatei sichern

Nachdem Sie nun auf **X1000** eine funktionierende Konfiguration erstellt haben, sollten Sie diese sichern:

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

Ein weiteres Menüfenster erscheint:

X1000 Setup Tool	BinTec Communications AG
[EXIT]: Exit Setup	MyX1000
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 **X1000** mit dem Login-Prompt. Alle Änderungen, die Sie vorher mit dem Setup Tool durchgeführt haben, sind gesichert. Beim nächsten Starten von **X1000** 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 **X1000** mit dem Login-Prompt. Alle Änderungen, die Sie vorher mit dem Setup Tool durchgeführt haben, gehen beim Ausschalten von **X1000** verloren.

7 Weiterführende Konfiguration

In diesem Kapitel finden Sie weitere Möglichkeiten zur Konfiguration von **X1000** für den fortgeschrittenen Benutzer. Wenn Sie zusätzliche Einstellungen machen wollen, die mit dem Configuration Wizard bzw. dem [Kapitel 6, Seite 135](#) nicht abgedeckt werden, dann sind Sie hier richtig.

Folgende Konfigurationsschritte werden erläutert:

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



Nutzen Sie die Funktion Taschengeldkonto (siehe [Kapitel 8.1.3, Seite 317](#)). Damit können Sie für Verbindungen mit **X1000** ein Limit festlegen, um Gebühren aufgrund von Fehlern bei der Konfiguration in Grenzen zu halten.

7.1 Allgemeine WAN-Einstellungen

Allgemeine WAN-Funktionen:

- **X1000** als dynamischer IP-Adreß-➤➤ **Server**
- ➤➤ **CAPI** User Concept
- Allgemeine ➤➤ **PPP**-Einstellungen

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

7.1.1 Dynamic IP Address Server

IP-Adreß-Pools **X1000** 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 **X1000** zunächst, ob für den Anrufer in der Routing-Tabelle eine Host-Route eingetragen ist. Wenn dies nicht der Fall ist, kann **X1000** eine IP-Adresse aus einem Adreß-Pool zuweisen (falls verfügbar).



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

Die Konfiguration erfolgt in:

- **IP ➤ 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 7-1: **IP ► IP ADDRESS POOL WAN (PPP)**

Feld	Bedeutung
IP Transit Network	Legt fest, ob zwischen X1000 und WAN-Partner ein Transitnetzwerk verwendet werden soll. Bei Zuweisung eines Adreß-Pools muß hier <i>dynamic server</i> ausgewählt werden.

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

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

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

ToDo Gehen Sie folgendermaßen vor:

- Gehen Sie zu **IP ► 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**.

7.1.2 CAPI User Concept

Benutzername und Paßwort Das CAPI User Concept erlaubt eine Kontrolle über den Zugriff auf den CAPI-Dienst. Damit wird erreicht, daß nur Benutzer, die mit Benutzername und Paßwort eingetragen sind, die CAPI-Dienste von **X1000** 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 [Kapitel 6.1.4, Seite 146](#)), 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 7-4: **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 X1000 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 X1000 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> : Datenruf <input type="checkbox"/> <i>voice</i> : Sprach-Ruf <input type="checkbox"/> <i>any</i> : beliebiger Ruf

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

Wenn sich beim Starten von **X1000** in **CAPI** ➔ **USER** kein Eintrag befindet, wird automatisch ein Standardeintrag ohne Paßwort erzeugt (mit **Name** = *default* und **CAPI** = *enabled*).

ToDo Gehen Sie folgendermaßen vor:

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

- Geben Sie **Password** ein.
- Wählen Sie **CAPI** aus: *enabled*.
- 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 **Eingabetaste** oder fügen Sie einen neuen Eintrag mit **ADD** hinzu.
- Wählen Sie **Item** aus: *CAPI*.



Falls Sie auf Ihrem Rechner mit einer Kommunikationsanwendung arbeiten, die auf Remote CAPI 1.1 aufsetzt (aktuell: Remote CAPI 2.0), muß **X1000** 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.

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

7.1.3 Allgemeine PPP-Einstellungen

Authentisierung ➤➤ PPP-Einstellungen, die z. B. zur Authentisierung der Verbindungspartner mit ➤➤ CHAP oder ➤➤ PAP erforderlich sind, tragen Sie bei jedem WAN-Partner ein (siehe [Kapitel 6.2.1, Seite 169](#)). Wenn ein Ruf eingeht, erkennt **X1000** 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 **X1000** keine Calling Line Number an. Eine Identifizierung des Anrufers via CLID kann also nicht erfolgen, auch wenn der Anrufer als WAN-Partner eingetragen ist. **X1000** weiß nicht, mit welchem ➤➤ **PPP-Authentisierungsprotokoll** er den eingehenden Ruf identifizieren kann.

Allgemeine PPP-Einstellungen Um eine Rufannahme trotzdem zu ermöglichen, führt **X1000** 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 **X1000** 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>none</i>: keine PPP-Authentisierung
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.

Tabelle 7-6: **PPP**

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

- Gehen Sie zu **PPP**.
- Wählen Sie **Authentication Protocol** aus, z. B. *CHAP + PAP + MS-CHAP*.
- Wählen Sie **PPP Link Quality Monitoring** aus, z. B. *no*.
- Bestätigen Sie mit **SAVE**.

7.1.4 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> <p><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.</p> <p><i>Packet Switch</i> stellen Sie ein, wenn Sie die X.31-TEI für den X.25-Router nutzen möchten.</p>

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

7.2 WAN-Partner-spezifische Einstellungen

Spezielle Funktionen für **➤➤ WAN-Partner** ermöglichen, die Eigenschaften für Verbindungen zu WAN-Partnern individuell festzulegen. Die beschriebenen Konfigurationsschritte nehmen Sie für jeden WAN-Partner separat vor.

- Delay after Connection Failure ([Kapitel 7.2.1, Seite 223](#))
- Channel Bundling - Basiskonfiguration für Wählverbindungen ([Kapitel 7.2.2, Seite 224](#))
- Channel Bundling - Bandwidth on Demand (BOD) - erweiterte Konfiguration für PPP-Verbindungen ([Kapitel 7.2.3, Seite 226](#))
- Always On/Dynamic ISDN (AO/DI) ([Kapitel 7.2.4, Seite 233](#))
- Layer 1 Protocol ([Kapitel 7.2.5, Seite 247](#))
- IP Transit Network ([Kapitel 7.2.6, Seite 249](#))
- Übermittlung von DNS- und WINS-Server-IP-Adressen an WAN-Partner ([Kapitel 7.2.7, Seite 253](#))
- **➤➤ RIP** ([Kapitel 7.2.8, Seite 256](#))
- Komprimierung: **➤➤ VJHC**, **➤➤ STAC**, MS-STAC ([Kapitel 7.2.9, Seite 259](#))
- **➤➤ Proxy ARP** ([Kapitel 7.2.10, Seite 261](#))
- Keepalive Monitoring ([Kapitel 7.2.11, Seite 263](#))

Im folgenden werden die jeweils erforderlichen Konfigurationsschritte genau erläutert.

7.2.1 Delay after Connection Failure

Mit dieser Funktion richten Sie eine Wartezeit nach fehlgeschlagenem Verbindungsversuch durch **X1000** 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 X1000 unternommen wird.

Tabelle 7-8: **WAN PARTNER** ► **EDIT** ► **ADVANCED SETTINGS**

ToDo Gehen Sie folgendermaßen vor:

- Gehen Sie zu **WAN PARTNER** ► **EDIT** ► **ADVANCED SETTINGS**.
- Geben Sie **Delay after Connection Failure (sec)** ein.
- Bestätigen Sie mit **OK**.
- Bestätigen Sie mit **SAVE**.

7.2.2 Channel Bundling - Basiskonfiguration für Wählverbindungen

X1000 unterstützt dynamische und statische ►► **Kanalbündelung** für Wählverbindungen über Multilink PPP.

Dynamisch Bei dynamischer Kanalbündelung wird beim Aufbau einer Verbindung zunächst nur ein B-Kanal geöffnet. **X1000** schaltet bei Bedarf, also bei großem Datendurchsatz, den zweiten ►► **ISDN-B-Kanal** für Verbindungen mit dem WAN-Partner zu, um die Bandbreite zu erhöhen. Sinkt das Datenaufkommen, wird der zweite ►► **B-Kanal** wieder geschlossen.

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.

Statisch Bei statischer Kanalbündelung legen Sie von vorneherein fest, daß **X1000** zwei B-Kanäle für Verbindungen mit dem WAN-Partner nutzen soll, unabhängig von der übertragenen Datenmenge.

Beide B-Kanäle werden in einem Zeitraum kleiner 1 Sekunde initiiert.

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 Verbindung geöffnet sind. Mögliche Werte: 1, 2.

Tabelle 7-9: **WAN PARTNER** ► **EDIT** ► **ADVANCED SETTINGS**

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

Mögliche Werte	Bedeutung
<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 7-10: **Channel Bundling**

ToDo Gehen Sie folgendermaßen vor:

- Gehen Sie zu **WAN PARTNER** ➤ **EDIT** ➤ **ADVANCED SETTINGS**.
- Wählen Sie **Channel Bundling** aus: *dynamic* oder *static*.
- Geben Sie **Total Number of Channels** ein.
- Bestätigen Sie mit **OK**.
- Bestätigen Sie mit **SAVE**.

Beachten Sie auch die erweiterten Konfigurationsoptionen (Bandwidth on Demand, BOD), siehe [Kapitel 7.2.3, Seite 226](#).

7.2.3 Channel Bundling - Bandwidth on Demand (BOD) - erweiterte Konfiguration für PPP-Verbindungen

Bandbreitenmanagement, im folgenden als BOD (Bandwidth on Demand) bezeichnet, bietet im Vergleich zur Basiskonfiguration (siehe [Kapitel 7.2.2, Seite 224](#)) erweiterte Konfigurationsoptionen für Wählverbindungen. Darüber hinaus können Sie bei hohem Datenfluß mit Hilfe von BOD Festverbindungen mit Wählverbindungen dynamisch bündeln. Sie können auch auf einfache Weise einen Backup-Modus für Festverbindungen konfigurieren, sodaß eine Wählverbindung zum Partner aufgebaut wird, falls die Festverbindung ausfällt.

Sie haben zusätzlich die Möglichkeit, eine etwaige Verwendung des Bandwidth Allocation Control Protocols (BACP/BAP nach RFC 2125) festzulegen.

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

Die Konfiguration von BOD erfolgt in

- **WAN PARTNER** ► **EDIT** ► **ADVANCED SETTINGS** ► **EXTENDED INTERFACE SETTINGS (OPTIONAL)**
- **WAN PARTNER** ► **EDIT** ► **WAN NUMBERS** ► **ADD** (Beschreibung des Menüs in [Kapitel 6.2, Seite 167](#))
- **WAN PARTNER** ► **EDIT** ► **PPP** (Beschreibung des Menüs in [Kapitel 6.2, Seite 167](#))

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



Die im folgenden beschriebenen Felder erscheinen für Wählverbindungen bzw. für Festverbindungen nur unter bestimmten Voraussetzungen.

Für Wählverbindungen erscheinen die Felder nur, wenn vorher im Menü **WAN PARTNER** ► **EDIT** ► **ADVANCED SETTINGS** unter **Channel Bundling** *dynamic* und im Menü **WAN PARTNER** ► **EDIT** ► **ADVANCED SETTINGS** ► **EXTENDED INTERFACE SETTINGS** unter **Mode** *Bandwidth On Demand Enabled* ausgewählt wurde.

Für Festverbindungen erscheinen die Felder nur, wenn vorher im Menü **WAN PARTNER** ► **EDIT** ► **ADVANCED SETTINGS** ► **EXTENDED INTERFACE SETTINGS** unter **Mode** z. B. *Bandwidth On Demand Active* ausgewählt wurde.



Die Voreinstellungen in den Feldern **Line Utilization Weighting**, **Line Utilization Sample (sec)**, **Gear Up Threshold** und **Gear Down Threshold** sollten nur für spezielle Anwendungen verändert werden. Für Standardanwendungen empfehlen wir, die voreingestellten Werte zu verwenden; sie entsprechen denen der Basiskonfiguration (siehe [Kapitel 7.2.2, Seite 224](#)).

Feld	Bedeutung
Mode	Legt fest, welcher Modus für BOD verwendet wird. Mögliche Werte: siehe Tabelle 7-12 , Seite 232 .
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 in Prozent, ab der bei einer Verbindung ein weiterer B-Kanal zugeschaltet wird. Ein B-Kanal wird zugeschaltet, wenn der aktuelle Durchsatz der entsprechenden Schnittstelle zum Verbindungspartner für mindestens 5 Sekunden Gear Up Threshold oder mehr beträgt.

Feld	Bedeutung
Gear Down Threshold	B-Kanäle werden weggeschaltet, bis die verbleibenden Kanäle mindestens den hier verbleibenden Auslastungsgrad in Prozent aufweisen. Ein B-Kanal wird abgeschaltet, wenn der berechnete Wert 10 Sekunden lang Gear Down Threshold der übrigbleibenden Kanäle unterschreitet.
D-Channel Queue Length	(nur bei Layer 1 Protocol = AO/DI im Menü WAN PARTNER ► EDIT ► ADVANCED SETTINGS) Schwellwert für die im D-Kanal angesammelte Anzahl von Bytes, ab der in den B-Kanal-Modus gewechselt werden soll (siehe Kapitel 7.2.4, Seite 233).
Maximum Number of Dialup Channels	Maximal erlaubte Anzahl der Kanäle, die geöffnet werden. Für Wählverbindungen wird der Wert an dieser Stelle nur angezeigt, eingestellt wird er im Menü WAN PARTNER ► EDIT ► ADVANCED SETTINGS unter Total Number of Channels . Für Festverbindungen kann der Wert an dieser Stelle eingestellt werden.

Tabelle 7-11: **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>	<p>Im Active Mode zeigt BAP folgendes Verhalten:</p> <ul style="list-style-type: none"> ■ Call-Request: einer der beiden Kommunikationspartner möchte einen B-Kanal zuschalten; wird gegebenenfalls initiiert. ■ Callback-Request: die Gegenseite wird aufgefordert, einen B-Kanal zuzuschalten; wird nicht initiiert aber gegebenenfalls akzeptiert. ■ Link-Drop-Request: ein Kommunikationspartner möchte einen B-Kanal abbauen; der Abbau wird gegebenenfalls initiiert oder akzeptiert. <p><i>BAP, Active Mode</i> ist erforderlich für die Funktion AO/DI (Always On/Dynamic ISDN), siehe Tabelle 7-17, Seite 241</p>

Mögliche Werte	Bedeutung
<i>BAP, Passive Mode</i>	<p>Im Passive Mode zeigt BAP folgendes Verhalten:</p> <ul style="list-style-type: none"> ■ Call-Request: einer der beiden Kommunikationspartner möchte einen B-Kanal zuschalten; wird gegebenenfalls akzeptiert. ■ Callback-Request: die Gegenseite wird aufgefordert, einen B-Kanal zuzuschalten; wird gegebenenfalls initiiert. ■ Link-Drop-Request: ein Kommunikationspartner möchte einen B-Kanal abbauen; der Abbau wird gegebenenfalls initiiert oder akzeptiert.
<i>BAP, Active and Passive Mode</i>	<p>Im Active and Passive Mode zeigt BAP folgendes Verhalten:</p> <ul style="list-style-type: none"> ■ Call-Request: einer der beiden Kommunikationspartner möchte einen B-Kanal zuschalten; wird gegebenenfalls initiiert oder akzeptiert. ■ Callback-Request: wird nicht verwendet. ■ Link-Drop-Request: ein Kommunikationspartner möchte einen B-Kanal abbauen; der Abbau wird gegebenenfalls initiiert oder akzeptiert.
<i>BAP, Client Active Mode</i>	<p>Im Client Active Mode zeigt BAP folgendes Verhalten:</p> <p>Der Partner, der den initialen Call aufbaut, befindet sich im <i>Active Mode</i> (siehe <i>BAP, Active Mode</i>), der Partner, der den initialen Call annimmt im <i>Passive Mode</i> (siehe <i>BAP, Passive Mode</i>).</p>

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

Tabelle 7-12: **Mode**

ToDo Gehen Sie folgendermaßen vor:

- Gehen Sie zu **WAN PARTNER** ➤ **EDIT** ➤ **ADVANCED SETTINGS** ➤ **EXTENDED INTERFACE SETTINGS (OPTIONAL)**.
- Wählen Sie **Mode** und **Line Utilization Weighting** aus.
- Tragen Sie **Line Utilization Sample (sec)** und bei Festverbindungen **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**.

7.2.4 Always On/Dynamic ISDN (AO/DI)

Always On/Dynamic ISDN (AO/DI) nutzt die bereits vorhandene ISDN-Infrastruktur, um ohne Hardware-Änderungen einen neuen Dienst für den Nutzer einzurichten: AO/DI stellt eine ständig verfügbare (always on) aber dennoch kostengünstige Verbindung vom Endkunden zum 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 **X1000** 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). Dieser Wechsel in den B-Kanal-Modus bzw. die Zuschaltung eines weiteren B-Kanals kann einerseits auf Basis der Durchsatzmessung erfolgen oder andererseits getriggert über Pakete von IP-basierenden Applikationen. Auf **X1000** 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 [Kapitel 8.2.8, Seite 338](#)). Mit Hilfe dieser Re-

geln 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 **X1000** 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 236](#))
- X.25 Konfiguration durchführen (siehe "[X.25-Konfiguration](#)", [Seite 236](#)):
 - Link-Konfiguration für Datex-P
 - Call-Routing
- AO/DI-Partner als WAN-Partner anlegen (siehe "[AO/DI-Partner als WAN-Partner anlegen](#)", [Seite 238](#))
 - 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 **X1000** 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 236](#)).

Im folgenden finden Sie alle notwendigen Schritte, um **X1000** mit dem Setup Tool für AO/DI zu konfigurieren:

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

- Gehen Sie zu **CM-1BRI, ISDN S0** ➤ **ADVANCED SETTINGS** (das Menü ist beschrieben in [Kapitel 7.1.4, Seite 222](#)).
- Wählen Sie **X.31 TEI Value** aus: *specify*.



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

- 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 unter 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 7-13: X.25 ► LINK CONFIGURATION ► EDIT

- Wählen Sie **L3 Packet Size max** aus: *256*.
- Wählen Sie **WindowSize/Packetsize Neg.** aus: *never*.
- Geben Sie **Highest Two-Way-Channel (HTC)** ein: *1*.
- Bestätigen Sie mit **SAVE**.
- Verlassen Sie **X.25 ► LINK CONFIGURATION** mit **Exit**.

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

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

Folgende 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 7-14: X.25 ► ROUTING ► ADD

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

AO/DI-Partner als WAN-Partner anlegen

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

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

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

- Gehen Sie zu **WAN PARTNER** ➤ **ADD** ➤ **PPP**.
- Wählen Sie **Authentication** aus, z. B. *CHAP*.
- Überspringen Sie **Partner PPP ID**.
- Geben Sie **Local PPP ID** ein, z. B. *bintec_router*.
- Geben Sie zweimal **PPP Password** ein, z. B. *secret*.
Bei Eingabe des Paßworts erscheint auf dem Bildschirm für jeden Buchstaben ein Sternchen als Platzhalter.
- Bestätigen Sie mit **OK**.

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

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

Folgender Teil des Menüs ist für diesen Konfigurationsschritt relevant:

Feld	Bedeutung
Layer 1 Protocol	Legt fest, welches Layer 1 Protocol X1000 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. Mögliche Werte bei X1000 : 1 oder 2.
Remote X.25 Address	X.25-Zieladresse. Erscheint nur, wenn unter Layer 1 Protocol <i>AO/DI</i> ausgewählt ist.

Tabelle 7-15: **WAN PARTNER** ► **ADD** ► **ADVANCED SETTINGS**

- Wählen Sie **Layer 1 Protocol** aus: *AO/DI*.
- Geben Sie **Total Number of Channels** ein, z. B. 1.
- Geben Sie **Remote X.25 Address** ein, z. B. 019011.

Regelung des durchsatzgesteuerten Bandbreitenmanagements

Gehen Sie folgendermaßen vor, um BACP/BAP für den "AO/DI-Client"-Zugang zu konfigurieren:

- 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 (siehe Tabelle 7-11, Seite 229).
Line Utilization Sample (sec)	Länge des Intervalls, über welches die gemessenen Durchsatzdaten gemittelt und mit Line Utilization Weighting gewichtet werden.
Gear Up Threshold	Auslastung in Prozent, ab der bei einer Verbindung ein weiterer B-Kanal zugeschaltet wird. Ein B-Kanal wird zugeschaltet, wenn der aktuelle Durchsatz der entsprechenden Schnittstelle zum Verbindungspartner für mindestens 5 Sekunden Gear Up Threshold oder mehr beträgt.
Gear Down Threshold	B-Kanäle werden weggeschaltet, bis die verbleibenden Kanäle mindestens den hier verbleibenden Auslastungsgrad in Prozent aufweisen. Ein B-Kanal wird abgeschaltet, wenn der berechnete Wert 10 Sekunden lang Gear Down Threshold der übrigbleibenden Kanäle unterschreitet.
D-Channel Queue Length	Schwellwert für die im D-Kanal angesammelte Anzahl von Bytes, ab der in den B-Kanal-Modus gewechselt werden soll.
Maximum Number of Dialup Channels	Maximale Anzahl der Kanäle, die geöffnet werden dürfen. Der Wert wird unter WAN PARTNER ➤ ADD ➤ ADVANCED SETTINGS im Feld Total Number of Channels festgelegt.

Tabelle 7-16: **WAN PARTNER** ➤ **ADD** ➤ **ADVANCED SETTINGS** ➤ **EXTENDED INTERFACE SETTINGS (OPTIONAL)**

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

Mögliche Werte	Bedeutung
<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; wird gegebenenfalls initiiert. ■ Callback-Request: die Gegenseite wird aufgefordert, einen B-Kanal zuzuschalten; wird nicht initiiert aber gegebenenfalls akzeptiert. ■ Link-Drop-Request: ein Kommunikationspartner möchte einen B-Kanal abbauen; der Abbau wird gegebenenfalls initiiert oder akzeptiert.

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

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

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

- Gehen Sie zu **WAN PARTNER** ➤ **ADD** ➤ **WAN NUMBERS** ➤ **ADD**.
- Geben Sie **Number** ein, z. B.: *0911123456*.
- Wählen Sie **Direction** aus: *outgoing*.
- Bestätigen Sie mit **SAVE**.

- Verlassen Sie **WAN PARTNER** ➤ **ADD** ➤ **WAN NUMBERS** ➤ **ADD** mit **Exit**.

Bei dynamischer Vergabe der IP-Adresse seitens des 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 8.2.8, Seite 338](#)). 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 8.2.8, Seite 338](#)). 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 8.2.8, Seite 338](#)) 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. Mögliche Werte bei X1000 : 1 oder 2.

Tabelle 7-18: **IP** ➤ **BANDWIDTH ON DEMAND (BOD)** ➤ **RULES FOR BOD** ➤ **ADD**

Das Feld **Action**, das angibt, wie mit einem ausgefilterten Datenpaket verfahren werden soll, enthält folgende Auswahlmöglichkeiten:

Mögliche Werte	Bedeutung
<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 7-19: **Action**

- Wählen Sie **Action** aus, z. B. *Invoke M*.
- Wählen Sie **Direction** aus, z. B. *outgoing*.
- Wählen Sie **Number of Channels** aus, z. B. *1*.
- Wählen Sie **Filter** aus, z. B. *mail_smtp_out*.
- Bestätigen Sie mit **SAVE**.
- Verlassen Sie **IP** ➤ **BANDWIDTH ON DEMAND (BOD)** ➤ **RULES FOR BOD** mit **Exit**.
- Verlassen Sie **IP** ➤ **BANDWIDTH ON DEMAND (BOD)** mit **Exit**.
Sie befinden sich wieder im Hauptmenü.

Um eine Regel auf ein Interface anzuwenden, gehen Sie folgendermaßen vor:

- Gehen Sie zu **IP** ➤ **BANDWIDTH ON DEMAND (BOD)** ➤ **CONFIGURE INTERFACES FOR BOD**.
- Wählen Sie das Interface aus, auf das Sie eine Regel anwenden möchten, z. B. *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 **X1000** 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**.

7.2.5 Layer 1 Protocol (ISDN-B-Kanal)

ISDN-B-Kanal Sie können das Layer 1 Protocol des ISDN-➤➤ **B-Kanals**, das **X1000** für Verbindungen zum WAN-Partner nutzen soll, definieren. Voreingestellt ist das Protokoll für ISDN-Datenverbindungen mit 64 kBit/s, was der Standardwert 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 X1000 nutzen soll. Diese Einstellung gilt nur für ausgehende Rufe an den WAN-Partner und für eingehende Rufe vom WAN-Partner, wenn sie anhand der Calling Party's Number identifiziert werden konnten.

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



Für eingehende Rufe, die nicht anhand der Calling Party's Number identifiziert werden können, verwendet X1000 als Layer 1 Protocol die Einstellungen unter **Item** in **CM-1BRI, ISDN S0** ► **INCOMING CALL ANSWERING** (siehe [Kapitel 6.1.4, Seite 146](#)).

Layer 1 Protocol enthält folgende Auswahlmöglichkeiten:

Mögliche Werte	Bedeutung
<i>ISDN 64 kbps</i>	Für ISDN-Datenverbindungen mit 64 kBit/s. Dies ist der Standardwert.
<i>ISDN 56 kbps</i>	Für ISDN-Datenverbindungen mit 56 kBit/s.
<i>Modem</i>	Auf X1000 nicht verfügbar.
<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 Bit/s, 2400 Bit/s, ..., 38400 Bit/s.
<i>Modem Profile 1 ... 8</i>	Auf X1000 nicht verfügbar.
<i>PPTP PNS</i>	Für VPN-Schnittstelle.
<i>AO/DI</i>	Für die Nutzung von Always On / Dynamic ISDN (AO/DI, siehe Kapitel 7.2.4, Seite 233)

Tabelle 7-21: **Layer 1 Protocol**



Die meisten Einträge von **Layer 1 Protocol** entsprechen den Einträgen von **Item** in **CM-1BRI, ISDN S0** ► **INCOMING CALL ANSWERING** (siehe [Kapitel 6.1.4, Seite 146](#)).

ToDo Gehen Sie folgendermaßen vor:

- Gehen Sie zu **WAN PARTNER** ► **EDIT** ► **ADVANCED SETTINGS**.
- Wählen Sie **Layer 1 Protocol** aus.

- Bestätigen Sie mit **OK**.
- Bestätigen Sie mit **SAVE**.

7.2.6 IP Transit Network

Wenn Sie einen WAN-Partner auf **X1000** eintragen, gibt es verschiedene Möglichkeiten, die IP-Adresse des Partners bzw. Partnernetzes anzugeben:

- Sie geben ➤➤ **IP-Adresse** und ➤➤ **Netzmaske** des Partners bzw. Partnernetzes an. Dazu müssen Sie diese natürlich kennen.
- Sie verwenden sowohl für **X1000** 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.

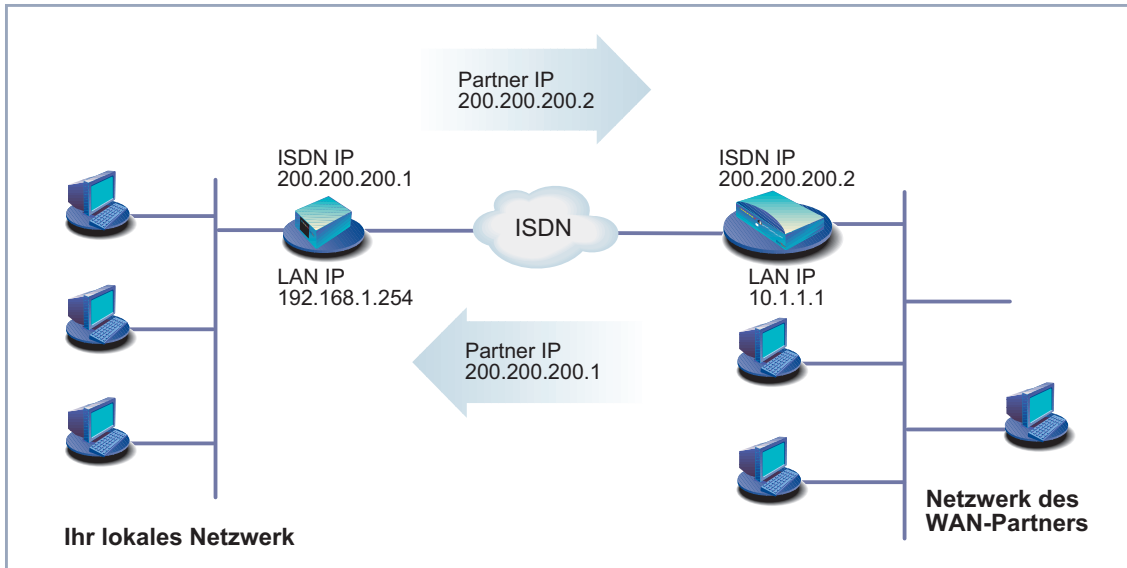


Bild 7-1: LAN-LAN-Kopplung mit Transitnetzwerk

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

Feld	Bedeutung
IP Transit Network	Legt fest, ob X1000 ein Transitnetzwerk zum WAN-Partner nutzt.
local IP Address	<p>IP-Adresse von X1000.</p> <p>Erscheint nur bei folgenden Werten für IP Transit Network: <i>no, dynamic client, dynamic server</i>.</p> <p>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.</p>
local ISDN IP Address	ISDN-IP-Adresse von X1000 im Transitnetzwerk.
Partner's ISDN IP Address	ISDN-IP-Adresse des WAN-Partners im Transitnetzwerk.
Partner's LAN IP Address	IP-Adresse des LAN Ihres WAN-Partners bzw. LAN-IP-Adresse (Host).
Partner's LAN Netmask	Netzmaske des LAN Ihres WAN-Partners. Wenn Sie keinen Eintrag machen, trägt X1000 eine Standardnetzmaske für die unter Partner's LAN IP Address verwendete Netzklasse ein.

Tabelle 7-22: **WAN PARTNER** ► **EDIT** ► **IP**

IP Transit Network enthält folgende Auswahlmöglichkeiten:

Mögliche Werte	Bedeutung
<i>yes</i>	Verwendung eines Transitnetzwerkes.
<i>dynamic client</i>	X1000 erhält seine IP-Adresse für die Dauer der Verbindung vom WAN-Partner.
<i>dynamic server</i>	X1000 weist dem Remote-WAN-Partner für die Dauer der Verbindung eine IP-Adresse zu. Dazu muß X1000 als dynamischer IP-Adreß-Server konfiguriert sein, d. h. über einen IP-Adreß-Pool verfügen (siehe Kapitel 7.1.1, Seite 214).
<i>no</i>	Kein Transitnetzwerk. Für die meisten WAN-Partner ist diese Einstellung ausreichend.

Tabelle 7-23: **IP Transit Network**

ToDo Gehen Sie folgendermaßen vor:

- Gehen Sie zu **WAN PARTNER** ➤ **EDIT** ➤ **IP**.
- Wählen Sie **IP Transit Network** aus.
- Geben Sie gegebenenfalls **local IP Address** ein (kein Transitnetzwerk).
- Geben Sie gegebenenfalls **local ISDN IP Address** ein (Transitnetzwerk).
- Geben Sie gegebenenfalls **Partner's ISDN IP Address** ein (Transitnetzwerk).
- Geben Sie gegebenenfalls **Partner's LAN IP Address** ein.
- Geben Sie gegebenenfalls **Partner's LAN Netmask** ein.
- Bestätigen Sie mit **SAVE**.

7.2.7 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 Ihren primären Domain Name Server gerichtet wird, versucht er, die Namensauflösung mit Hilfe seiner internen Tabellen zu erreichen. Falls er den Namen nicht findet, fragt er bei einem ihm bekannten übergeordneten Domain Name Server nach.



Falls Sie die Funktion DNS Proxy nutzen, kann **X1000** u. a. einmal aufgelöste Namen und IP-Adressen im Cache speichern und überprüft bei einer Anfrage zunächst, ob die gesuchte Adresse aus dem Cache beantwortet werden kann. Damit werden die Kosten, die durch Aufbau von WAN-Verbindungen zu Name Servern außerhalb des LANs entstehen, niedrig gehalten und die Performance im LAN optimiert, da Anfragen an häufig genutzte oder schon einmal aufgelöste Adressen von **X1000** selbst beantwortet werden. Die Konfiguration des DNS Proxy finden Sie in [Kapitel 7.3.2, Seite 273](#).

Bei Eintragen eines WAN-Partners auf **X1000** können Sie festlegen, ob **X1000** 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 X1000s erstem globalen Domain Name Server (DNS).
Secondary Domain Name Server	IP-Adresse eines weiteren globalen Domain Name Servers.
Primary WINS	IP-Adresse von X1000s erstem globalen WINS (Windows Internet Name Server) bzw. NBNS (NetBIOS Name Server).
Secondary WINS	IP-Adresse eines weiteren globalen WINS bzw. NBNS.

Tabelle 7-24: *IP* ➤ *STATIC SETTINGS*

Feld	Bedeutung
Dynamic Name Server Negotiation	Legt fest, ob X1000 IP-Adressen für Primary Domain Name Server , Secondary Domain Name Server , Primary WINS und Secondary WINS im Falle einer dynamischen Name-Server-Aushandlung vom WAN-Partner erhält oder an den WAN-Partner sendet.

Tabelle 7-25: *WAN PARTNER* ➤ *EDIT* ➤ *IP* ➤ *ADVANCED SETTINGS*

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

Mögliche Werte	Bedeutung
<i>off</i>	X1000 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"> ■ X1000 sendet Anfragen nach Name-Server-Adressen an den WAN-Partner, falls <i>dynamic client</i> ausgewählt ist. ■ X1000 beantwortet Anfragen des WAN-Partners nach Name-Server-Adressen vom WAN-Partner, falls <i>dynamic server</i> ausgewählt ist. ■ X1000 beantwortet, aber sendet keine Anfragen nach Name-Server-Adressen, falls <i>yes</i> oder <i>no</i> ausgewählt ist.
<i>client (receive)</i>	X1000 sendet Anfragen nach Name-Server-Adressen an den WAN-Partner.
<i>server (send)</i>	X1000 beantwortet Anfragen des WAN-Partners nach Name-Server-Adressen.

Tabelle 7-26: **Dynamic Name Server Negotiation**

WINS, DNS im LAN Falls Sie einen Domain Name Server bzw. Windows Internet Name Server in Ihrem LAN eingerichtet haben, geben Sie dessen IP-Adresse an.

ToDo Gehen Sie dazu folgendermaßen vor, falls Sie diese Eintragung nicht schon gemacht haben ([Kapitel 7.3.2, Seite 273](#)):

- 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 **X1000** die eingetragenen DNS- bzw. WINS-Server-IP-Adressen dem WAN-Partner mitteilen soll (Server-Modus) bzw. wenn bei Verbindungen zum WAN-Partner andere DNS/WINS-Adressen als im LAN verwendet werden sollen (Client-Modus, z. B. bei Einwahl zu einem Internet Service Provider).

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



Wenn Sie keinen Secondary DNS bzw. WINS Server haben, können Sie ein zweites Mal die IP-Adresse des Primary DNS bzw. WINS Server 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. Genaue Informationen dazu in [Kapitel 3.7.2, Seite 73](#).

7.2.8 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 [Kapitel 6.2.1, Seite 169](#)) entscheidet der Router, auf welchem Weg (Route) er das Datenpaket weiter-schickt, 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. **X1000** 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. **X1000** kann beides.

WAN-Partner Wenn Sie mit einem WAN-Partner Empfangen und/oder Senden von RIP-Paketen vereinbaren, kann **X1000** 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 **X1000** verändern können.

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

Die Konfiguration erfolgt in:

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

■ **CM-BNC/TP, ETHERNET** ► **ADVANCED SETTINGS**

Feld	Bedeutung
RIP Send	Ermöglicht Senden von RIP-Paketen über die Schnittstelle zum WAN-Partner bzw. die LAN-Schnittstelle.
RIP Receive	Ermöglicht Empfangen von RIP-Paketen über die Schnittstelle zum WAN-Partner bzw. die LAN-Schnittstelle.

Tabelle 7-27: **WAN PARTNER** ► **EDIT** ► **IP** ► **ADVANCED SETTINGS** bzw. **CM-BNC/TP, 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 7-28: **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-BNC/TP, ETHERNET** ➤ **ADVANCED SETTINGS**.
- Wählen Sie **RIP Send** aus.
- Wählen Sie **RIP Receive** aus.
- Bestätigen Sie mit **SAVE**.

7.2.9 Komprimierung

Datenkomprimierung Mit Hilfe von ➤➤ **Datenkomprimierung** können Sie den Datendurchsatz erhöhen und damit die Verbindungskosten senken. **X1000** unterstützt mehrere Möglichkeiten, abhängig von der gewählten ➤➤ **Enkapsulierung**, z. B. PPP (siehe [Kapitel 6.2.1, Seite 169](#)):

■ ➤➤ **STAC**

Durch den in **X1000** 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 **X1000** 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 7-29: **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).
<i>MPPC</i>	Auf X1000 nicht verfügbar.

Tabelle 7-30: **Compression**

Feld	Bedeutung
Van Jacobson Header Compression	Ermöglicht VJHC.

Tabelle 7-31: **WAN PARTNER** ► **EDIT** ► **IP** ► **ADVANCED SETTINGS**

STAC, MS-STAC Gehen Sie folgendermaßen vor, um STAC oder MS-STAC einzustellen:

- Gehen Sie zu **WAN PARTNER** ► **EDIT**.
- Wählen Sie **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**.

7.2.10 Proxy ARP (Address Resolution Protocol)

ARP-Requests Mit Hilfe von ➤➤ **Proxy ARP** kann **X1000** ➤➤ **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 **X1000** Proxy ARP aktiviert ist und der gewünschte Host über eine definierte WAN-Verbindung erreichbar ist, beantwortet **X1000** den ARP Request mit seiner eigenen Hardware-Adresse. Dies ist für den Verbindungsaufbau ausreichend: Die ➤➤ **Datenpakete** werden an **X1000** geschickt, der sie dann an den gewünschten Host weiterleitet.

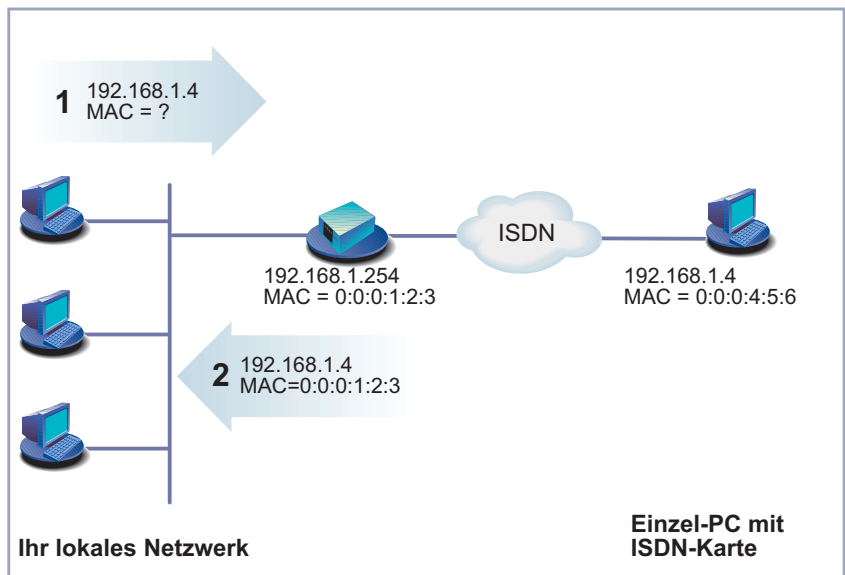


Bild 7-2: Proxy ARP

Die Konfiguration erfolgt in:

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

■ **CM-BNC/TP, ETHERNET** ➤ **ADVANCED SETTINGS**

Feld	Bedeutung
Proxy Arp	Ermöglicht X1000 , ARP Requests zu beantworten.

Tabelle 7-32: **WAN PARTNER** ➤ **EDIT** ➤ **IP** ➤ **ADVANCED SETTINGS** bzw. **CM-BNC/TP, 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>	X1000 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> baut X1000 nach dem ARP Request eine Verbindung auf.
<i>on (up only)</i>	X1000 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 7-33: **Proxy Arp**

Proxy Arp in **CM-BNC/TP, 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 7-34: **Proxy Arp**

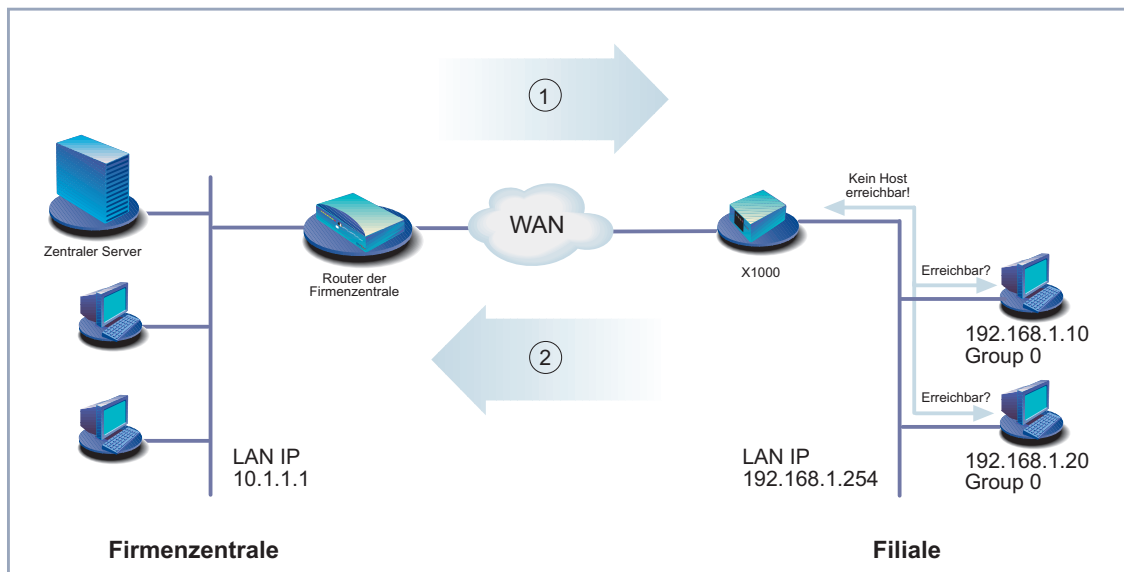
ToDo Gehen Sie folgendermaßen vor:

- Gehen Sie zu **WAN PARTNER** ► **EDIT** ► **IP** ► **ADVANCED SETTINGS**.
- Wählen Sie **Proxy Arp** aus.
- Bestätigen Sie mit **OK**.
- Bestätigen Sie mit **SAVE**.
- Bestätigen Sie mit **SAVE**.
- Verlassen Sie **WAN PARTNER** mit **EXIT**.
Sie befinden sich wieder im Hauptmenü.
- Gehen Sie zu **CM-BNC/TP, ETHERNET** ► **ADVANCED SETTINGS**.
- Wählen Sie **Proxy Arp** aus.
- Bestätigen Sie mit **SAVE**.
- Bestätigen Sie mit **SAVE**.

7.2.11 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 7-3, Seite 264](#)), befindet sich häufig ein zentraler Server im LAN der Firmenzentrale. Wenn dieser zentrale Server so konfiguriert ist, daß er regelmäßig WAN-Verbindungen zu **X1000** 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	X1000 ist "besetzt", keine Verbindung möglich
---	----------------------------------	---	--

Bild 7-3: Keepalive Monitoring

Kosten senken Mit der Funktion Keepalive Monitoring können Sie **X1000** in der Filiale so konfigurieren, daß unnötige WAN-Verbindungen von der Firmenzentrale zur Filiale vermieden werden. In regelmäßigen, einstellbaren Abständen überprüft **X1000**, 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 **X1000** 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 **X1000** 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 **X1000** die erneute Erreichbarkeit signalisiert, ist abhängig vom eingestellten Überwachungsintervall (**Interval**).



Der entsprechende WAN-Partner, also z. B. die Firmenzentrale, sollte auf **X1000** per CLID (Calling Line Identification) identifiziert werden können. Wenn dies nicht der Fall ist, kann Keepalive Monitoring u. U. unwirksam sein.

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

Feld	Bedeutung
Group	<p>Definiert eine Gruppe von Hosts, deren Erreichbarkeit von X1000 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 X1000 überwacht werden soll.</p>
Interval	<p>Definiert ein Zeitintervall in Sekunden, 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 X1000 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 X1000-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 Schnittstellenbereiches auf X1000, 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 X1000 konfigurierten WAN-Partner (Wählverbindung). Die Indizes anderer Schnittstellen finden Sie in der Software Reference.</p>
Range	<p>Definiert den Bereich von Schnittstellen auf X1000, 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 7-35: **SYSTEM** ► **KEEPALIVE MONITORING** ► **ADD**

In **SYSTEM** ► **KEEPALIVE MONITORING** sind alle Hosts aufgelistet, die per Keep-alive Monitoring überwacht werden. Unter **State** ist dabei die Erreichbarkeit der Hosts aufgelistet: *alive*, wenn der Host bei der letzten Überprüfung erreichbar war, *down*, wenn er nicht erreichbar war.

ToDo Gehen Sie folgendermaßen vor, um das in [Bild 7-3, Seite 264](#) dargestellte Beispiel zu konfigurieren:

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

- Drücken Sie **ADD**, um den ersten Host hinzuzufügen, der mit Keepalived Monitoring von **X1000** 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: **10001**.
- 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: **10001**.
- Geben Sie **Range** ein, **4999**.
- Bestätigen Sie mit **SAVE**.

Mit diesen Einstellungen erreichen Sie, daß **X1000** 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 **X1000** für Wählverbindungen zu WAN-Partnern deaktiviert. Die Überprüfung der Hosts durch **X1000** geht mit dem Zeitintervall 300 s weiter und sobald mindestens einer wieder erreichbar ist, reaktiviert **X1000** die Schnittstellen.

7.3 Grundlegende IP-Einstellungen

Hier finden Sie einige grundlegende Einstellungen, die Sie auf **X1000** festlegen können:

- Beziehen der Systemzeit
- Namensauflösung (➤➤ **DNS**) auf **X1000**
- ➤➤ **Port**-Nummern
- ➤➤ **BOOTP** Relay Agent

Im folgenden werden die jeweils erforderlichen Konfigurationsschritte erläutert.

7.3.1 Systemzeit

Systemzeit Die Systemzeit benötigen Sie, um korrekte Zeitstempel bei der Aufzeichnung von Verbindungsdaten (Accounting) zu erhalten.

Sie können die Systemzeit

- automatisch beziehen, z. B. über ISDN oder über einen Time Server (siehe "[Systemzeit automatisch beziehen](#)", Seite 270).
- manuell auf **X1000** einstellen (siehe "[Systemzeit manuell einstellen](#)", Seite 273).

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 zur bezogenen Zeit addiert oder von ihr subtrahiert wird. Wenn Sie Werte zwischen -24 und +24 eingeben, versteht X1000 die Angabe als Anzahl von Stunden und wandelt sie nach dem Drücken von SAVE automatisch in die entsprechende Anzahl von Sekunden um.</p> <p>Beachten Sie: Wenn Sie <i>ISDN</i> als Time Protocol wählen, müssen Sie den Time Offset auf 0 setzen. Sie benötigen in diesem Fall keinen Time Offset, weil Sie automatisch die korrekte Zeit der jeweiligen Zeitzone erhalten.</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 X1000 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 = <i>TIME/UDP</i> , <i>TIME/TCP</i> oder <i>SNTP</i> : Aktuelle Zeit wird alle Time Update Interval Sekunden überprüft. Bei Time Protocol = <i>ISDN</i> : Aktuelle Zeit wird jeweils bei der ersten ISDN-Verbindung nach Ablauf von Time Update Interval überprüft.
Time Server	IP-Adresse des Time- »» Servers , den X1000 nutzt. Time Server wird nicht benötigt, wenn Sie <i>ISDN</i> als Time Protocol einstellen.

Tabelle 7-36: 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 7-37: **Time Protocol**

ISDN Gehen Sie folgendermaßen vor, um die Systemzeit über ISDN zu beziehen:

- »»** Gehen Sie zu **IP **»» STATIC SETTINGS****.

- Wählen Sie **Time Protocol** aus: *ISDN*.
- Geben Sie **Time Offset (sec)** ein: *0*.
- Geben Sie **Time Update Interval (sec)** ein, z. B. *86400* (entspricht 24 Stunden).
- Bestätigen Sie mit **SAVE**.

Mit der ersten ISDN-Verbindung bezieht **X1000** die Systemzeit über ISDN.

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

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

X1000 bezieht somit die Systemzeit über einen Time Server. Alle 24 Stunden gleicht **X1000** 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 **X1000** 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 X1000 eingestellte Systemzeit an (Datum und Uhrzeit).
New Time:	Hier wird die neue Uhrzeit eingegeben, die X1000 verwenden soll (Stunden:Minuten).
New Date:	Hier wird das neue Datum eingegeben, das X1000 verwenden soll (Monat/Tag/Jahr).

Tabelle 7-38: **SYSTEM** ➤ **TIME AND DATE**

Gehen Sie folgendermaßen vor, um die Systemzeit auf **X1000** manuell einzugeben:



Wenn auf **X1000** zusätzlich eine Methode zum automatischen Beziehen der Zeit festgelegt ist, haben die auf diese Weise erhaltenen Werte höhere Priorität. D. h. falls **X1000** ein entsprechendes Zeitsignal erhält (z. B. von einem Time Server), wird eine evtl. manuell eingegebene Systemzeit überschrieben.

- Gehen Sie zu **SYSTEM** ➤ **TIME AND DATE**.
- Geben Sie **New Time** ein.
- Geben Sie **New Date** ein.
- Bestätigen Sie die neue Systemzeit mit **SET**.
Unter **Current Time:** wird die auf **X1000** neu eingestellte Systemzeit angezeigt.

7.3.2 Namensauflösung - X1000 mit DNS Proxy

Wozu Namensauflösung?

IP-Adresse = ? Namensauflösung ist erforderlich, um Host-Namen in einem LAN oder im Internet in IP-Adressen zu übersetzen. Wenn Sie also z. B. den Host "Goofy" in Ihrem LAN ansprechen möchten (z. B. mit telnet oder ping) oder die **URL** "http://www.bintec.de" in Ihren Internet Browser eingeben, benötigen Sie jeweils die dazugehörige IP-Adresse, um die geforderte Verbindung aufbauen zu können. Dazu gibt es im allgemeinen verschiedene Möglichkeiten, z. B.:

- **DNS (Domain Name Service):**
Auf einem DNS Server werden zu Host-Namen die entsprechenden IP-Adressen in Form von DNS Records hinterlegt und bei einer entsprechenden Anfrage aufgelöst, d. h. ein DNS Record mit der zum Namen gehörigen IP-Adresse wird vom Name Server an die Quelle der Anfrage geschickt. Name Server bilden eine hierarchische Baumstruktur. Wenn also ein Name Server einen Namen nicht auflösen kann, fragt er bei einem übergeordneten Name Server nach usw.
- **HOSTS-Dateien (siehe [Kapitel 3.7.2, Seite 73](#)):**
Auf HOSTS-Dateien, die sich auf den PCs im LAN befinden, legen Sie eine Tabelle von Host-Namen mit den dazugehörigen IP-Adressen an. Damit sind zur Auflösung dieser Namen Verbindungen zu DNS Servern überflüssig. Da man die Aktualisierung der HOSTS-Dateien auf jedem PC durchführen muß, ist diese Methode zur Namensauflösung ziemlich arbeitsaufwendig.

In der Praxis wird zur Namensauflösung häufig der DNS Server des Internet Service Providers genutzt.

Vorteile der Namensauflösung mit X1000

X1000 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 **X1000** 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 **X1000** als DNS Server auf den entsprechenden Rechnern eintragen können. DNS-Anfragen werden vom Rechner an **X1000** 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 **X1000** als DHCP Server zugewiesen bekommen.

Durch Forwarding-Einträge kann **X1000** entscheiden, welcher DNS Server zur Auflösung bestimmter Namen herangezogen werden soll. Wenn Sie also z. B. auf **X1000** 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 **X1000** 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 **X1000** gespeichert. Wenn also ein einmal aufgelöster Name erneut benötigt wird, kann **X1000** die Anfrage aus dem Cache beantworten, eine Anfrage an einen externen Name Server ist nicht erneut nötig. Damit können diese Anfragen schneller beantwortet werden, Bandbreite auf den WAN-Verbindungen und Kosten für unnötige Verbindungen werden eingespart.

Wenn eine DNS-Anfrage von keinem der befragten DNS Server beantwortet werden kann, wird dies im Cache als negativer dynamischer Eintrag gespeichert. Da fehlgeschlagene, also nicht zu beantwortende, DNS-Anfragen in der Regel von Applikationen oder IP-Stacks nicht gespeichert werden, können diese im Cache gespeicherten negativen dynamischen Einträge häufige, erfolglose Verbindungsaufbauten zu externen DNS Servern verhindern.

Die Gültigkeit der positiven dynamischen Einträge im Cache ergibt sich aus der TTL (Time To Live), die im DNS Record enthalten ist. Negativen Einträgen wird der Wert **Maximum TTL for Neg Cache Entries** zugewiesen. Nach Ablauf der TTL wird ein dynamischer Eintrag aus dem Cache gelöscht.

Statische Namenseinträge

Mit positiven statischen Einträgen geben Sie auf **X1000** Namen mit den dazugehörigen IP-Adressen ein. Wenn Sie auf diese Weise häufig benötigte IP-Adressen speichern, kann **X1000** entsprechende DNS-Anfragen selbst beantworten, die Verbindung zu einem externen Name Server ist nicht nötig. Damit wird der Zugriff auf diese Adressen beschleunigt. Für ein kleines Netzwerk kann so ein Name Server auf **X1000** eingerichtet werden, die Installation eines separaten DNS Servers bzw. die umständliche Pflege von HOSTS-Dateien auf den Rechnern im LAN ist nicht erforderlich.

Bei negativen statischen Einträgen wird einem Namen keine IP-Adresse zugeordnet, eine entsprechende DNS-Anfrage wird negativ beantwortet und auch an keinen anderen Name Server weitergeleitet.



Einen dynamischen Eintrag können Sie in **IP** ➔ **DNS** ➔ **DYNAMIC CACHE** ganz einfach per "Knopfdruck" in einen statischen umwandeln (siehe [Tabelle 7-43, Seite 287](#)).

Filterfunktion

Durch Verwendung von negativen statischen Einträgen können Sie die Namensauflösung auf **X1000** 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 **X1000** auf eine entsprechende DNS-Anfrage antwortet.



Achten Sie bei Ihren statischen Einträgen darauf, daß diese immer auf dem aktuellsten 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 **X1000** oder durch einen anderen Name Server aufgelöst wird (siehe [Kapitel 12.1, Seite 410](#)). Hilfe zu dem Kommando erhalten Sie durch Eingabe von `nslookup -?`.

Weitere Möglichkeiten

Globale Name Server Desweiteren können Sie unter **IP** ► **STATIC SETTINGS** die IP-Adresse von globalen Name Servern eintragen, die bevorzugt befragt werden sollen, wenn **X1000** Anfragen nicht selbst oder durch Forwarding-Einträge beantworten kann.

Für lokale Anwendungen kann als globaler Name Server die IP-Adresse von **X1000** oder die Loopback-Adresse (127.0.0.1) eingetragen werden.

Die Adressen von Name Servern kann **X1000** 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 Name-Server-Verhandlung eine Verbindung aufgebaut wird, wenn eine Namensauflösung durch die bereits genannten Methoden nicht erfolgreich war.

Austausch von DNS-Server-Adressen mit LAN-Partnern

DHCP Wenn **X1000** als DHCP Server konfiguriert ist, können den DHCP Clients im LAN IP-Adressen von Name Servern übermitteln werden. Dabei können die Adressen der auf **X1000** eingetragenen globalen Name Server übermitteln werden oder die Adresse von **X1000** selbst. Im letzteren Fall gehen DNS-Anfragen

von den DHCP Clients an **X1000**, 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 Name Servern aktiviert ist und **X1000** im Server-Modus arbeitet (**Dynamic Name Server Negotiation = server (send)**). In diesem Fall können bei Name-Server-Verhandlungen über IPCP mit dem WAN-Partner, der IP-Adreß-Client ist, ebenfalls die Adressen der globalen Name Server oder die Adresse von **X1000** selbst übermittelt werden.

Wenn **X1000** im Client-Modus arbeitet (**Dynamic Name Server Negotiation = client (receive)**), können gegebenenfalls Name Server-Adressen mit dem WAN-Partner, der IP-Adreß-Server ist, ausgehandelt und an **X1000** übermittelt werden. Diese können als globale Name Server auf **X1000** eingetragen werden und somit für zukünftige Namensauflösungen zur Verfügung stehen.

Strategie zur Namensauflösung auf X1000

Eine DNS-Anfrage wird von **X1000** folgendermaßen behandelt:

1. Kann die Anfrage aus dem statischen oder dynamischen Cache direkt beantwortet werden (IP-Adresse oder negative Antwort)?
 - Falls ja, wird die Information weitergeleitet.
 - Falls nein, siehe 2.
2. Ist ein passender Forwarding-Eintrag vorhanden?
In diesem Fall werden die entsprechenden DNS Server befragt. Falls die Verbindung zum WAN-Partner nicht aktiv ist, wird versucht, sie aufzubauen.
 - Falls ein DNS Server den Namen auflösen kann, wird die Information weitergeleitet und ein dynamischer Eintrag im Cache erzeugt.
 - Falls keiner der befragten DNS Server den Namen auflösen kann oder kein passender Forwarding-Eintrag vorhanden ist, siehe 3.
3. Sind globale Name Server eingetragen?
In diesem Fall werden die entsprechenden DNS Server befragt. Ist für lokale Anwendungen die IP-Adresse von **X1000** oder die Loopback-Adresse eingetragen, werden diese hier ignoriert.

- Falls ein DNS Server den Namen auflösen kann, wird die Information weitergeleitet und ein dynamischer Eintrag im Cache erzeugt.
 - Falls keiner der befragten DNS Server den Namen auflösen kann oder keine statischen Name Server eingetragen sind, siehe 4.
4. Ist ein WAN-Partner als Default Interface ausgewählt?
In diesem Fall werden die dazugehörigen DNS Server befragt. Falls die Verbindung zum WAN-Partner nicht aktiv ist, wird versucht, sie aufzubauen.
- Falls ein DNS Server den Namen auflösen kann, wird die Information weitergeleitet und ein dynamischer Eintrag im Cache erzeugt.
 - Falls keiner der befragten DNS Server den Namen auflösen kann oder kein Default Interface ausgewählt wurde, siehe 5.
5. Ist das Überschreiben der Adressen der globalen Name Server zulässig (**Overwrite Global Nameserver** = yes)?
In diesem Fall wird eine Verbindung zum ersten WAN-Partner aufgebaut, der so konfiguriert ist, daß Adressen von DNS Servern übermittelt werden könnten – soweit dies vorher noch nicht versucht wurde. Bei erfolgreicher Name-Server-Aushandlung werden diese als globale Name Server eingetragen und stehen somit für weitere Anfragen zur Verfügung.
6. Anfrage wird mit 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 Negativeintrag aufgenommen.

Konfiguration – Überblick

Die Konfiguration und Überwachung der Namensauflösung auf **X1000** 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 X1000s Domain Name fest.
Primary Domain Name Server	IP-Adresse von X1000s erstem globalen Domain Name Server (DNS).
Secondary Domain Name Server	IP-Adresse eines weiteren globalen Domain Name Servers.
Primary WINS	IP-Adresse von X1000s erstem globalen WINS (Windows Internet Name Server) bzw. NBNS (NetBIOS Name Server).
Secondary WINS	IP-Adresse eines weiteren globalen WINS bzw. NBNS.

Tabelle 7-39: **IP ➤ STATIC SETTINGS**

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 Name Servern auf X1000 (in IP ► STATIC SETTINGS) mit von WAN-Partnern übermittelten Name-Server-Adressen überschrieben werden dürfen. 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 Name-Server-Verhandlung aufgebaut wird, wenn andere Versuche zur Namensauflösung nicht erfolgreich waren.</p>
DHCP Assignment	<p>Legt fest, welche Name-Server-Adressen dem DHCP Client übermittelt werden, wenn X1000 als DHCP Server konfiguriert ist. Mögliche Werte:</p> <ul style="list-style-type: none"> ■ <i>none</i>: Es wird keine Name-Server-Adresse übermittelt. ■ <i>self</i> (Standardwert): Es wird die Adresse von X1000 als Name-Server-Adresse übermittelt. ■ <i>global</i>: Es werden die Adressen der auf X1000 eingetragenen globalen Name Server übermittelt.

Feld	Bedeutung
IPCP Assignment	<p>Legt fest, welche Name-Server-Adressen von X1000 bei einer dynamischen Name-Server-Verhandlung an einen WAN-Partner übermittelt werden. Mögliche Werte:</p> <ul style="list-style-type: none">■ <i>none</i>: Es wird keine Name-Server-Adresse übermittelt.■ <i>self</i>: Es wird die Adresse von X1000 als Name-Server-Adresse übermittelt.■ <i>global</i> (Standardwert): Es werden die Adressen der auf X1000 eingetragenen globalen Name Server übermittelt.
Static Hosts	In Klammern wird die Anzahl der statischen Einträge angezeigt.
Forwarded Domains	In Klammern wird die Anzahl der Forwarding-Einträge angezeigt.
Dynamic Cache	In Klammern wird die Anzahl der positiven und negativen dynamischen Einträge im DNS Cache angezeigt.

Tabelle 7-40: IP ➔ DNS

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

Feld	Bedeutung
Default Domain	Der in IP ➤ STATIC SETTINGS eingetragene Domain Name von X1000 wird angezeigt.
Name	<p>Host-Name, 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 zugehörige 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>)</p> <p>IP-Adresse, die Name zugeordnet wird.</p>
TTL	<p>Gültigkeitsdauer der Zuordnung von Name zu Address in Sekunden (nur relevant bei Response = <i>positive</i>). Dieser Wert wird dem TTL-Feld (Time To Live) gegeben, falls X1000 einen entsprechenden DNS Record verschickt.</p> <p>Standardwert: <i>86400</i> (= 24 h)</p>

Tabelle 7-41: **IP** ➤ **DNS** ➤ **STATIC HOSTS** ➤ **ADD**

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

Feld	Bedeutung
Global Nameservers:	Die in IP ➤ STATIC SETTINGS eingetragenen globalen Name Server werden angezeigt.
Default Domain:	Der in IP ➤ STATIC SETTINGS eingetragene Domain Name von X1000 wird angezeigt.
Name	Host-Name, der mit diesem Forwarding-Eintrag aufgelöst werden soll. Kann auch Wildcards enthalten (nur am Anfang von Name , z. B. *.bintec.de). Bei Eingabe eines unvollständigen Namens ohne Punkt wird dieser nach Bestätigung mit SAVE mit ".Default Domain" vervollständigt.
Interface	Legt den WAN-Partner fest, zu dem zur Auflösung von Name eine Verbindung aufgebaut wird.
TTL	Gültigkeitsdauer der Zuordnung von Name zu Address in Sekunden. Standardwert: 86400 (= 24 h) Wenn die Anfrage von X1000 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 X1000 in der Regel nicht verändert wird. Falls das erhaltene TTL-Feld den Wert 0 hat oder Maximum TTL for Pos Cache entries überschreitet, wird dem weitergeleiteten DNS Record TTL mitgegeben.

Tabelle 7-42: **IP** ➤ **DNS** ➤ **FORWARDED DOMAINS** ➤ **ADD**

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

Feld	Bedeutung
Name	Host-Name, dem Address mit diesem dynamischen Eintrag im Cache zugeordnet wird.
Address	IP-Adresse, die Name zugeordnet wird.
Resp	<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 7-43: **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 7-44: **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 Name Server weitergeleitet wurden.
Cache Hitrate (%)	Zeigt die Anzahl von Cache Hits pro DNS Requests in Prozent an.
Successfully Answered Queries	Zeigt die Anzahl der erfolgreich (positiv und negativ) beantworteten Anfragen an.
Server Failures	Zeigt die Anzahl der Anfragen an, die kein Name Server (weder positiv noch negativ) beantworten konnte.

Tabelle 7-45: **IP** ► **DNS** ► **GLOBALS STATISTICS...**

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

Feld	Bedeutung
Dynamic Name Server Negotiation	Legt fest, ob X1000 IP-Adressen für Primary Domain Name Server , Secondary Domain Name Server , Primary WINS und Secondary WINS im Falle einer dynamischen Name-Server-Aushandlung vom WAN-Partner erhält oder an den WAN-Partner sendet.

Tabelle 7-46: **WAN PARTNER** ➤ **EDIT** ➤ **IP** ➤ **ADVANCED SETTINGS**

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

Mögliche Werte	Bedeutung
<i>off</i>	X1000 sendet und beantwortet keine Anfragen nach Name-Server-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"> ■ X1000 sendet Anfragen nach Name-Server-Adressen an den WAN-Partner, falls <i>dynamic client</i> ausgewählt ist. ■ X1000 beantwortet Anfragen des WAN-Partners nach Name-Server-Adressen vom WAN-Partner, falls <i>dynamic server</i> ausgewählt ist. ■ X1000 beantwortet, aber sendet keine Anfragen nach Name-Server-Adressen, falls <i>yes</i> oder <i>no</i> ausgewählt ist.
<i>client (receive)</i>	X1000 sendet Anfragen nach Name-Server-Adressen an den WAN-Partner.
<i>server (send)</i>	X1000 beantwortet Anfragen des WAN-Partners nach Name-Server-Adressen.

Tabelle 7-47: **Dynamic Name Server Negotiation**

Konfiguration – Vorgehensweise

ToDo Gehen Sie folgendermaßen vor, um Namensauflösung mit dem DNS Proxy auf **X1000** zu konfigurieren:

Namensauflösung auf X1000 Tragen Sie gegebenenfalls zunächst globale Name Server auf **X1000** ein:

- Gehen Sie zu **IP** ► **STATIC SETTINGS**.
- Geben Sie **Domain Name** ein, z. B. **mycompany.com**.

- Geben Sie gegebenenfalls **Primary** bzw. **Secondary Domain Name Server** ein.
- Geben Sie gegebenenfalls **Primary** bzw. **Secondary WINS** ein.



Wenn Sie keinen Secondary DNS bzw. Secondary WINS Server haben, können Sie ein zweites Mal die IP-Adresse des Primary DNS bzw. WINS Servers in das Feld **Secondary Domain Name Server** bzw. **Secondary WINS** eingeben.

Dies kann für die Verbindung mit manchen DFÜ-Clients notwendig sein.

- Bestätigen Sie mit **SAVE**.

Aktivieren bzw. deaktivieren Sie die Cache-Funktion und legen Sie allgemeine Einstellungen für den DNS Proxy fest:

- Gehen Sie zu **IP** ➤ **DNS**.
- Wählen Sie **Positive Cache** und **Negative Cache** aus, z. B. *enabled*.
- Wählen Sie **Overwrite Global Nameservers** aus, z. B. *yes*, wenn Sie unter **IP** ➤ **STATIC SETTINGS** keine globalen Name Server statisch eintragen wollen.
- Wählen Sie **DHCP Assignment** aus, z. B. *self*.
- Wählen Sie **IPCP Assignment** aus, z. B. *global*.

Legen Sie die Werte für die statischen und dynamischen Einträge fest:

- Gehen Sie zu **IP** ➤ **DNS** ➤ **ADVANCED SETTINGS...**
- Tragen Sie **Maximum Number of DNS Records** ein.
- Tragen Sie **Maximum TTL for Pos Cache entries** ein.
- Tragen Sie **Maximum TTL for Neg Cache Entries** ein.
- Bestätigen Sie mit **SAVE**.

So erzeugen Sie statische Einträge:

- Gehen Sie zu **IP** ➤ **DNS** ➤ **STATIC HOSTS**.
Hier sind alle vorhandenen statischen Einträge aufgelistet.
- Mit **ADD** 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**.

X1000 ↔ WAN-Partner

Wenn Sie einen WAN-Partner so konfigurieren möchten, daß die Adresse eines Name Servers gegebenenfalls von **X1000** an den WAN-Partner oder vom WAN-Partner an **X1000** übermittelt wird, gehen Sie folgendermaßen vor:

- Gehen Sie zu **WAN PARTNER** ➤ **EDIT** ➤ **IP** ➤ **ADVANCED SETTINGS**.
- Wählen Sie **Dynamic Name Server Negotiation** aus.
Hier nehmen Sie die gewünschte Einstellung vor.
- 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.

7.3.3 Port-Nummern

Was ist ein ➤➤ Port? **X1000** 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 **X1000** neben der IP-Adresse auch einen Port an. So wird die entsprechende Applikation angesprochen. Ports gibt es nur bei den Protokollen TCP und UDP!

X1000 leitet eingehende ➤➤ **Datenpakete** für die gewünschte Applikation an den Port mit der entsprechenden Nummer weiter. Damit wird die entsprechende Applikation von **X1000** angesprochen, die eingehenden Daten können verarbeitet werden.

In **IP** ➤ **STATIC SETTINGS** können Sie einige wichtige Port-Nummern 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 X1000 (siehe Kapitel 8.1.4, Seite 321) verhindert.

Tabelle 7-48: IP ► **STATIC SETTINGS**

ToDo Gehen Sie folgendermaßen vor, wenn Sie eine der Port-Nummern verändern wollen:

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

7.3.4 BOOTP Relay Agent

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

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

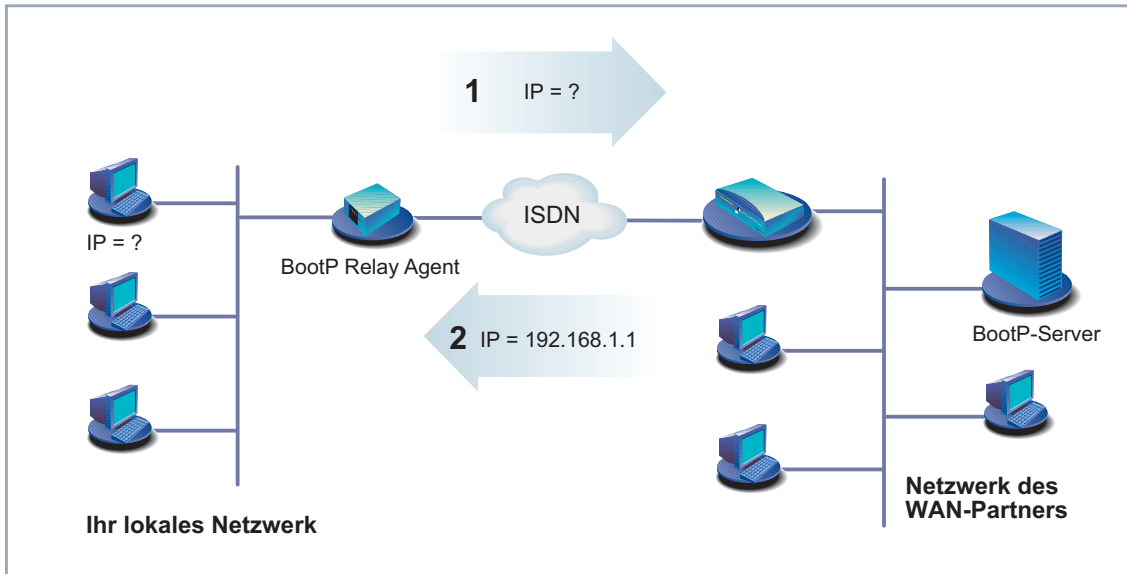


Bild 7-4: X1000 als BOOTP-Relay-Agent

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

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

Tabelle 7-49: **IP** ► **STATIC SETTINGS**

ToDo Gehen Sie folgendermaßen vor:

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



Wenn für die Verbindung zwischen BOOTP Server und BOOTP-Client eine ISDN-Verbindung erforderlich ist, muß ein entsprechender WAN-Partner eingerichtet sein (siehe [Kapitel 6.2.1, Seite 169](#)).

7.4 IPX-Einstellungen

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

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

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

7.4.1 Allgemeine Einstellungen

Hier finden Sie globale Parameter für IPX. Diese Einstellungen sind für alle IPX-Verbindungen von **X1000** gültig.

Die Konfiguration erfolgt in **IPX**:

Feld	Bedeutung
Local System Name	IPX-Systemname von X1000 . Dieser Name darf sich aus Großbuchstaben, Ziffern und den Zeichen <code>:/-</code> zusammensetzen.
Internal Network Number	X1000s interne Netzwerknummer. Dieser Wert muß unter allen Netzwerknummern einmalig sein und besteht standardmäßig aus den letzten vier Bytes von X1000s ➤ ➤ MAC-Adresse . Ändern Sie diesen Wert nur, wenn er bereits an anderer Stelle im Netzwerk verwendet wird.
enable IPX spoofing	Aktiviert bzw. deaktiviert NCP session watchdog ➤ ➤ Spoofing und die Behandlung von "broadcast message waiting"-Paketen. Mögliche Werte: <input type="checkbox"/> yes : kostengünstig für IPX-WAN-Verbindungen <input type="checkbox"/> no
enable SPX spoofing	Aktiviert bzw. deaktiviert SPX session watchdog spoofing. Mögliche Werte: <input type="checkbox"/> yes : kostengünstig für SPX-Sessions über WAN-Verbindungen <input type="checkbox"/> no
NetBIOS Broadcast replication	Definiert, wie X1000 mit ➤ ➤ NetBIOS -Paketen verfährt.

Tabelle 7-50: **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> <i>on LAN only</i>	Nur NetBIOS-Hosts im LAN, für die keine WAN-Verbindungen aufgebaut werden müssen, können aufeinander zugreifen. Kostengünstig.

Tabelle 7-51: **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**.

7.4.2 LAN-Schnittstelle konfigurieren

Konfigurieren Sie als nächstes die LAN-Schnittstelle von **X1000** 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 **X1000** diese Information nicht hat, kann er nicht aktiv am eigenen IPX-LAN teilnehmen.

Die Konfiguration erfolgt in **CM-BNC/TP, ETHERNET**.

Feld	Bedeutung
local IPX-NetNumber	Die IPX-Netzwerknummer des LANs, an das X1000 angeschlossen ist.
Encapsulation	Definiert, welche Art von Header bei IPX-Paketen im angeschlossenen LAN verwendet werden. Mögliche Werte: <ul style="list-style-type: none"> <input type="checkbox"/> <i>none</i> <input type="checkbox"/> <i>Ethernet II</i> <input type="checkbox"/> <i>Ethernet 802.2 LLC</i> <input type="checkbox"/> <i>Ethernet SNAP</i> <input type="checkbox"/> <i>Ethernet NOVELL 802.3</i>

Tabelle 7-52: **CM-BNC/TP, ETHERNET**

ToDo Gehen Sie folgendermaßen vor:

- Gehen Sie zu **CM-BNC/TP, ETHERNET**.
- Geben Sie **local IPX-NetNumber** ein.
- Wählen Sie **Encapsulation** aus.
- Bestätigen Sie mit **SAVE**.

7.4.3 WAN-Partner einrichten

Wenn die Verbindung zu 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. Bei Verbindungen zwischen X1000s genügt die Null.
Send RIP/SAP Updates	Definiert, wie oft ►► RIP -(Routing Information Protocol) und SAP - (Service Advertising Protocol) Pakete von X1000 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 7-53: **WAN PARTNER** ► **EDIT** ► **IPX**

Im Feld **Send RIP/SAP Updates** legen Sie fest, wie oft ►► **RIP**- und **SAP**-Pakete von **X1000** zum WAN-Partner geschickt werden. Das Feld 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 Standardeinstellung, 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 7-54: **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, z. B. *0*.
- Wählen Sie **Send RIP/SAP Updates** aus.

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

7.5 Funktionen mit Zusatzlizenz

In diesem Kapitel wird kurz dargestellt, welche Funktionen Sie auf **X1000** mit einer Zusatzlizenz freischalten können.

7.5.1 Virtual Private Network (VPN) und Verschlüsselung

Mit Hilfe von PPTP (Point to Point Tunneling Protocol) kann **X1000** ein VPN realisieren. Dies dient einer sicheren (verschlüsselten) Übertragung von Daten über WAN-Verbindungen, z. B. über das Internet. So kann von Außendienstmitarbeitern per Laptop ein Zugang auf Daten des Firmennetzes kostengünstig über das Internet realisiert werden (Einwahl über einen örtlichen Internet Service Provider).

Mit einer VPN-Lizenz sind implizit auch die Verschlüsselungsverfahren DES und Blowfish verfügbar (siehe [Kapitel 8.3.1, Seite 359](#)).

Detaillierte Informationen und Konfigurationshinweise (mit Beispielen) finden Sie in der Software Reference.

7.5.2 IPSec (Internet Protocol Security)

Der Sicherheitsstandard IPSec ermöglicht Ihnen, IP-basierte Daten sicher über öffentliche Netze (z. B. das Internet) auszutauschen.

Detaillierte Informationen und Konfigurationshinweise finden Sie im IPSec Reference Manual, das Sie zusammen mit Ihrer IPSec-Lizenz erhalten, bzw. in der Software Reference.

7.5.3 Festverbindungen (leased lines)

Mit einer Zusatzlizenz können Sie die ISDN-BRI-Schnittstelle von **X1000** nicht nur für Wählverbindungen sondern auch für Festverbindungen nutzen.

Konfigurationshinweise finden Sie in [Kapitel 6.1.4, Seite 146](#), und [Kapitel 6.2, Seite 167](#).

8 Sicherheitsmechanismen

SAFERNET BinTec Communications AG ermöglicht mit **X1000** eine hohe Sicherheit Ihres Netzwerks und Ihrer Verbindungen. Die verfügbaren Sicherheitsfunktionen (SAFERNET) erlauben das Überwachen von Aktivitäten über den Router und eine wirksame Zugangs- bzw. Abhörsicherung. Die erforderlichen Konfigurationsschritte werden in diesem Kapitel dargestellt.

Manches können Sie nicht mit Hilfe des Setup Tools konfigurieren, sondern nur durch direktes Eintragen in ►► **MIB**-Tabellen. Die entsprechenden Tabellen bzw. Variablen werden im jeweiligen Abschnitt genannt.



MIB-Einträge können Sie entweder durch Kommandos in der ►► **SNMP-Shell** oder durch externe SNMP-Manager, z. B. Configuration Manager, vornehmen. Eine Beschreibung der SNMP-Kommandos finden Sie in der Software Reference.

Das Kapitel ist folgendermaßen aufgebaut:

- Überwachen von Aktivitäten
- Zugangssicherung
- Abhörsicherung
- Besonderheiten
- Checkliste

8.1 Überwachen von Aktivitäten

Eine wesentliche Voraussetzung für einen hohen Grad an Sicherheit ist die Möglichkeit, alle Aktivitäten auf dem Router und über den Router hinweg beobachten zu können. Dazu stellt Ihnen BinTec Communications AG eine Vielzahl an Möglichkeiten zur Verfügung.

8.1.1 Syslog Messages

Alle wesentlichen Ereignisse auf **X1000**'s verschiedenen Subsystemen (►► ISDN, ►► PPP, ►► CAPI, usw.) werden in der Form von Syslog Messages (System logging messages) protokolliert.

Je nach eingestelltem Level (acht Stufen von critical über info bis debug) werden dabei mehr oder weniger viele Details sichtbar. Die protokollierten Daten werden intern auf **X1000** in einer Liste von einstellbarer Länge gespeichert. Alle Informationen können und sollten zur Speicherung und Weiterverarbeitung an einen oder mehrere externe Rechner weitergeleitet werden, z. B. an den Rechner des Systemadministrators. Auf **X1000** 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-BNC/TP-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 X1000 verbundenen Rechner. Verwenden Sie diese Einstellung nur, wenn Sie eine Fehleranalyse machen, da umfangreicher 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 Messages <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 X1000 intern gespeichert werden (Wertebereich: <i>0 - 1000</i>).</p>

Tabelle 8-1: **SYSTEM**

Feld	Bedeutung
Log Host	➤➤ IP-Adresse des Hosts, zu dem Syslog Messages weitergeleitet werden.
Level	Priorität der zu Log Host zu schickenden Syslog Messages. Entspricht Message level for the syslog table in SYSTEM .
Facility	Syslog Facility auf Log Host . Nur erforderlich, wenn der Log Host ein Unix-Rechner ist.
Type	Nachrichtentyp. Mögliche Werte: <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 8-2: **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 8-3: **CM-BNC/TP-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 8-4: **WAN PARTNER** ➤ **ADD** ➤ **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 **X1000** Accounting Messages von TCP-, UDP- und ICMP-Sitzungen bezüglich des ausgewählten LAN-Partners generiert und aufgezeichnet:

- Gehen Sie zu **CM-BNC/TP-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 **X1000** Accounting Messages von TCP-, UDP- und ICMP-Sitzungen gespeichert:

- Gehen Sie zu **WAN PARTNER** ➤ **EDIT** ➤ **IP** ➤ **ADVANCED SETTINGS**.
- Aktivieren Sie **IP Accounting** mit *on*.

Anzeigen von Syslog Messages Gehen Sie folgendermaßen vor, um Syslog Messages anzuzeigen:

- Gehen Sie zu **MONITORING AND DEBUGGING** ➤ **MESSAGES**.
Hier werden die auf **X1000** gespeicherten Syslog Messages angezeigt:


```

X1000 Setup Tool                               BinTec Communications AG
[MONITOR][MESSAGE]: Syslog Messages             MyX1000

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 **X1000** zu löschen.

Zur Interpretation von Syslog Messages: Siehe Software Reference.

8.1.2 Monitorfunktionen im Setup Tool

Neben Syslog Messages können Sie mit Hilfe des Setup Tools noch einige weitere Daten anzeigen. Dabei wird jeweils durch periodische Aktualisierung der aktuelle Status von bestimmten Teilsystemen dargestellt. Zu den folgenden Funktionsbereichen existieren Anzeigemodule:

- ISDN-Verbindungen
- Taschengeldkonto (Credits)
- Schnittstellenstatistik (vergleichende Darstellung mehrerer Schnittstellen)
- ➤➤ TCP/IP-Statistik
- Syslog Messages (siehe [Kapitel 8.1.1, Seite 308](#))

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.

X1000 Setup Tool			BinTec Communications AG			
[MONITOR][ISDN CALLS]: ISDN Monitor - Calls			MyX1000			
Dir	Remote Name/Number	Charge	Duration	Stack	Cannel	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 (Credits) Sie können den Stand des Taschengeldkontos für ISDN-Verbindungen oder für PPPoE-Verbindungen anzeigen lassen.

ISDN-Verbindungen Gehen Sie bei ISDN-Verbindungen folgendermaßen vor:

- 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.

X1000 Setup Tool		BinTec Communications AG	
[MONITOR][ISDN CREDITS][STAT]: Monitor isdnlogin Credits		MyX1000	
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		
Number of Current Incoming Connections	0		
Number of Current Outgoing Connections	0		
Number of Current Connections	0		
EXIT			

Informationen über die Konfiguration des Taschengeldkontos finden Sie in [Kapitel 8.1.3, Seite 317](#).

PPPoE-Verbindungen Gehen Sie folgendermaßen vor, um den Stand des Taschengeldkontos für PPPoE-Verbindungen anzeigen zu lassen:

- Gehen Sie zu **MONITORING AND DEBUGGING** ➤ **XDSL CREDITS** ➤ **PPPoE CREDITS**.

Der aktuelle Stand des Taschengeldkontos für PPPoE-Verbindungen wird angezeigt.

Schnittstellenstatistik Gehen Sie folgendermaßen vor, um aktuelle Werte und Aktivitäten der **X1000**-Schnittstellen anzuzeigen:

- Gehen Sie zu **MONITORING AND DEBUGGING** ➤ **INTERFACES**.

Die Werte von zwei Schnittstellen werden nebeneinander angezeigt.

X1000 Setup Tool		BinTec Communications AG		
[MONITOR][INTERFACE]: Interface Monitoring		MyX1000		
Interface Name	enl	PROVIDER		
Operational Status	up	dormant		
	total	per second	total	per second
Received Packets	5512	0	0	0
Received Octets	920664	0	0	0
Received Errors	0		0	
Transmit Packets	9	0	0	0
Transmit Octets	1193	0	0	0
Transmit Errors	0		0	
Active Connections	N/A		0	
Duration	N/A		0	
EXIT	EXTENDED		EXTENDED	

Use <Space> to select

- Wählen Sie unter **Interface Name** die anzuzeigende Schnittstelle aus.
- Wählen Sie **EXTENDED**, um zusätzliche Informationen anzuzeigen. Anschließend können Sie unter **Operation** den Status der Schnittstelle verändern und die Eingabe mit **START OPERATION** bestätigen.

TCP/IP-Statistik Gehen Sie folgendermaßen vor, um eine Statistik der Verbindungen mit den
 ➤➤ **Protokollen** ICMP, ➤➤ **IP**, UDP und TCP anzuzeigen:

- Gehen Sie zu **MONITORING AND DEBUGGING** ➤ **TCP/IP**.
 Die Statistik für IP-Verbindungen wird angezeigt. Die Bedeutung der MIB-Variablen finden Sie in der MIB Reference.

X1000 Setup Tool		BinTec Communications AG	
[MONITOR][IP]: IP Statistics		MyX1000	
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 statistische Daten zu ICMP darzustellen.
- Wählen Sie **i**, um statistische Daten zu IP darzustellen.
- Wählen Sie **u**, um statistische Daten zu UDP darzustellen.
- Wählen Sie **t**, um statistische Daten zu TCP darzustellen.

8.1.3 Taschengeldkonto (Credits Based Accounting System)

Credits Mit dem Taschengeldkonto von **X1000** übernehmen Sie u.a. die Kontrolle über anfallende Gebühren. Dadurch können Sie die Auswirkungen eventueller Konfigurationsfehler in Grenzen halten. Es ermöglicht Ihnen auch festzulegen, wieviele Verbindungen in einem bestimmten Zeitraum maximal anfallen dürfen. Sie können für bestimmte Subsysteme (➤➤➤ **PPP**, ➤➤➤ **CAPI**, ➤➤➤ **ISDN-Login**) Einstellungen vornehmen bezüglich der Anzahl der Verbindungen, der Verbindungszeit und der anfallenden ISDN-Verbindungsgebühren. Ist das festgelegte Limit überschritten, kann **X1000** innerhalb des festgelegten Zeitraums keine Verbindungen mehr aufbauen. So können Sie Konfigurationsfehler rechtzeitig erkennen, bevor Ihre Telefonrechnung sehr hoch ausfällt!

Syslog Messages Syslog Meldungen werden erzeugt bei Erreichen von 90% bzw. 100% des Limits und wenn die Taschengeldkonto-Funktion wegen überschrittenem Limit eine Verbindung verhindert.

Nach Aus- und wieder Einschalten bzw. Rebooten von **X1000** steht Ihnen wieder das gesamte Konto zur Verfügung.

Die Konfiguration erfolgt in **CREDITS** ► **ISDN CREDITS** bzw. in **CREDITS** ► **xDSL CREDITS** ► **PPPOE 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) ; erscheint nur bei ISDN-Verbindungen. 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) ; erscheint nur bei ISDN-Verbindungen. 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) ; erscheint nur bei ISDN-Verbindungen. 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; erscheint nur bei ISDN-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; erscheint nur bei ISDN-Verbindungen. Wenn Sie diese Einstellung mit <i>on</i> aktivieren, können Sie den gewünschten Wert in der darunterliegenden Zeile eintragen.

Tabelle 8-5: **CREDITS** ▶ **ISDN CREDITS** bzw. **CREDITS** ▶ **xDSL CREDITS** ▶ **PPPoE CREDITS**

ToDo Gehen Sie folgendermaßen vor, um ein Taschengeldkonto für ISDN-Verbindungen einzurichten:

- ▶ Gehen Sie zu **CREDITS** ▶ **ISDN CREDITS**.
- ▶ Wählen Sie ein 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**.

Gehen Sie folgendermaßen vor, um ein Taschengeldkonto für PPPoE-Verbindungen einzurichten:

- Gehen Sie zu **CREDITS** ➤ **xDSL CREDITS** ➤ **PPPoE CREDITS**.
- Wählen Sie **Surveillance** aus: *on*, wenn Sie das Taschengeldkonto nutzen wollen.
- Geben Sie **Measure Time (sec)** ein, z. B. *86400* (= 24 Stunden).
- Aktivieren Sie gegebenenfalls **Maximum Number of Outgoing Connections** und tragen Sie den gewünschten Wert ein.
- Aktivieren Sie gegebenenfalls **Maximum Time for Outgoing Connections (sec)** und tragen Sie den gewünschten Wert ein.
- Bestätigen Sie mit **SAVE**.

8.1.4 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 **X1000** anzeigen. So können alle


Benutzer des **X1000**-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 **X1000** eingeben.)

Die HTTP-Statusseite des BinTec-Routers mit dem Systemnamen `<System Name>` bzw. mit der angegebenen IP-Adresse wird angezeigt.

System Information: MyX1000 

System description

Type of System	X1000
System Name	MyX1000
Location	Germany
Contact	BINTEC
Software	V 5.1 Rev.4 from 2000/ 02/ 29 00:00:00
System state	up and running for 0d 0h 16min

Software options

ip	tunneling	stac	capi	ipz
o.k.	o.k.	o.k.	o.k.	o.k.

Hardware Interfaces

Slot	Interface	Status	Additional Info
Slot 1	Fast Ethernet	o.k.	
Slot 2	ISDN S0	o.k.	used 0, available 2

You can [update](#) this page, see a list of [system tables](#), or [login](#) to the router.

For more information about BinTec products see <http://www.bintec.de>

Bild 8-1: HTTP-Statusseite

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 **X1000**'s Subsystemen wird angezeigt.
- **Hardware Interfaces**
Hier werden die LAN- und WAN-Schnittstelle von **X1000** angezeigt. Die dritte Spalte der Tabelle informiert über den aktuellen Status der physikalischen Schnittstellen mit folgenden möglichen Werten:

Schnittstelle	Status	Mögliche Ursache
LAN (Slot 1)	o.k.	Normaler Betrieb.
	inactive	LAN-Kabel ist nicht angeschlossen.
WAN (Slot 2)	o.k.	Anzahl der verfügbaren sowie der momentan benutzten B-Kanäle wird angezeigt.
	unconfigured	ISDN-Kabel ist nicht angeschlossen oder ein falsches ►► D-Kanal -Protokoll ist eingetragen.

Tabelle 8-6: Status der Schnittstellen

Die HTTP-Statusseite enthält einige Links:

- **update**
Klicken Sie **update**, um die Statusseite zu aktualisieren.
- **login**
Klicken Sie **login**, um sich auf den dazugehörigen BinTec-Router via ►► **Telnet** einzuloggen.
- <http://www.bintec.de>
Damit gelangen Sie auf BinTecs WWW-Server mit den neuesten Informationen zu den Produkten sowie aktueller System-Software und Dokumentation für **X1000**.

- system tables

Klicken Sie auf system tables, um eine Liste mit allen MIB-Tabellen von **X1000** anzuzeigen. Durch Anklicken eines Tabellennamens werden die darin enthaltenen Variablen aufgelistet.



Wenn Sie die Anzeige von **X1000**'s HTTP-Statusseite verhindern möchten, dann tragen Sie als Port-Nummer des http-Ports 0 ein:

- Gehen Sie zu **IP** ➤ **STATIC SETTINGS**.
- Geben Sie **HTTP TCP port** ein: 0.
- Bestätigen Sie mit **SAVE**.

8.1.5 Activity Monitor

Wozu? Mit dem Activity Monitor können Windows-Nutzer die Aktivitäten von **X1000** 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 **X1000** ist möglich.

Wie funktioniert's? Ein Status-Daemon sammelt Informationen über **X1000** und überträgt sie in Form von UDP-Paketen zur Broadcast-Adresse des LAN (Standardeinstellung) oder zu einer explizit eingetragenen IP-Adresse. Ein Paket pro 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, solange die Paket-Größe von 4096 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 **X1000**(s) entsprechend konfigurieren
- die Windows-Anwendung auf Ihrem PC starten und verwenden (siehe bla bla BRICKware for Windows)

Die Konfiguration erfolgt in **SYSTEM** ➤ **EXTERNAL ACTIVITY MONITOR**:

Feld	Bedeutung
Client IP Address	<p>IP-Adresse, zu der X1000 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>Port-Nummer 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 8-7: **SYSTEM** ➤ **EXTERNAL ACTIVITY MONITOR**

ToDo Gehen Sie folgendermaßen vor:

- Gehen Sie zu **SYSTEM** ➤ **EXTERNAL ACTIVITY MONITOR**.
- Geben Sie **Client IP Address** ein, z. B. die IP-Adresse Ihres PCs.

- Geben Sie **Client UDP port** ein: *2107*.
- Wählen Sie **Type** aus, z. B. *physical_virt*.
- Geben Sie **Update Interval (sec)** ein, z. B. *5*.
- Bestätigen Sie mit **SAVE**.

8.2 Zugangssicherung

Es gibt einige Möglichkeiten, das Einloggen und Zugreifen auf **X1000** nur autorisierten Benutzern zu ermöglichen.

8.2.1 Anmelden

Paßwort Das Einloggen auf **X1000** kann wie in [Kapitel 5, Seite 111](#) 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 128](#) beschrieben.

- Ändern Sie unbedingt die Paßwörter, um unberechtigten Zugriff auf **X1000** zu verhindern.
- Achten Sie zusätzlich darauf, daß Unbefugte nicht auf die Stromzufuhr zu **X1000**, 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 **X1000** getrennt, wenn 15 Minuten lang keine Eingabe über die Tastatur erfolgt. Den Zeitraum können Sie mit dem Kommando `t <Zeit in Sekunden>` verändern (siehe [Kapitel 12.1, Seite 410](#)).



Wenn Sie ein Software Update durchführen (siehe [Kapitel 9.3, Seite 381](#)), sollten Sie den Autologout ausschalten: Geben Sie `t 0` in die SNMP-Shell ein.



Es ist möglich, zusätzliche Benutzer-Accounts mit Hilfe von SNMP-Kommandos anzulegen (siehe Software Reference). Einem Benutzer kann dabei ein bestimmtes Paßwort und eine bestimmte Aktion zugeordnet werden.

8.2.2 Überprüfen der eingehenden Rufnummer

CLID Mit Hilfe von Calling Line Identification (➤➤ **CLID**) überprüft **X1000** 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 **X1000** 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 **X1000** 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**.

8.2.3 Authentisierung von PPP-Verbindungen mit PAP, CHAP oder MS-CHAP

➤➤ **PAP**, ➤➤ **CHAP** und MS-CHAP sind die gebräuchlichen Verfahren zur Authentisierung von ➤➤ **PPP**-Verbindungen. Dabei werden durch ein standardisiertes Verfahren eine Benutzer-ID und ein Paßwort zur Überprüfung der Identität der Gegenstelle ausgetauscht. Weitere Informationen finden Sie in [Kapitel 6.2.1, Seite 169](#) und [Kapitel 7.1.3, Seite 220](#).

8.2.4 Callback

Rückruf Um zusätzliche Sicherheit bezüglich des Verbindungspartners zu erlangen oder die Kosten von Verbindungen eindeutig verteilen zu können, kann für jeden WAN-Partner der Callback-Mechanismus verwendet werden. Damit kommt eine Verbindung erst durch einen Rückruf zustande, nachdem der Anrufende eindeutig identifiziert wurde. **X1000** kann sowohl einen eingehenden Ruf mit einem Rückruf beantworten, also auch sich bei einem WAN-Partner einwählen und dann einen Rückruf erwarten:

Die Identifizierung kann aufgrund der Calling Party's Number oder aufgrund der PAP/CHAP/MS-CHAP-Authentisierung erfolgen. Im ersten Fall erfolgt die Identifikation ohne Rufannahme, da die Calling Party's Number über den ISDN-D-Kanal übermittelt wird, im zweiten Fall mit Rufannahme.



Weitere Informationen zum Callback-Mechanismus finden Sie in der Software Reference.

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

Feld	Bedeutung
Callback	Aktiviert die Funktion Callback.

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

Callback enthält folgende Auswahlmöglichkeiten:

Mögliche Werte	Bedeutung
<i>no</i>	X1000 führt keinen Rückruf aus.
<i>expected (awaiting callback)</i>	X1000 ruft den WAN-Partner an, um den Rückruf zu initiieren.
<i>yes (PPP negotiation)</i>	X1000 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)</i>	X1000 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 abzubrechen und die initiale Verbindung zu X1000 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 X1000 eingetragen ist, kann diese Abbruchoption nicht genutzt werden!
<i>yes</i>	X1000 ruft sofort zurück, wenn Ihr Router vom WAN-Partner dazu aufgefordert wird.

Tabelle 8-9: **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**.

8.2.5 Closed User Group

X1000 unterstützt die Nutzung des Dienstmerkmals "Geschlossene Benutzergruppe", das Sie bei Ihrer Telefongesellschaft für Ihren ISDN-Anschluß beantragen können. Damit wird die externe/interne Erreichbarkeit durch die Vermittlungsstellen überwacht und geregelt.

ToDo Gehen Sie folgendermaßen vor, um eine Geschlossene Benutzergruppe für einen WAN-Partner zu aktivieren:

- Gehen Sie zu **WAN PARTNER** ➤ **EDIT** ➤ **WAN NUMBERS** ➤ **EDIT** ➤ **ADVANCED SETTINGS**.
- Wählen Sie **Closed User Group** aus: *specify*.
- Geben Sie den CUG-Index ein.
- Bestätigen Sie mit **OK**.

8.2.6 Zugriff auf Remote CAPI

Zu den Besonderheiten der BinTec-Router gehört die Implementierung der Programmierschnittstellen ➤➤ **Remote CAPI** und Remote TAPI (nur bei PABX-Geräten). Dadurch können Applikationen auf Rechnern im LAN die Ressourcen des Routers nutzen, so als wären diese Komponenten direkt im Rechner eingebaut.

- CAPI User Concept** Durch Nutzung von BinTec's **▶▶ CAPI User Concept** können Sie sicherstellen, daß nur durch Benutzername und Paßwort authentifizierte Benutzer auf die Remote-CAPI-Schnittstelle von **X1000** zugreifen können (siehe [Kapitel 7.1.2, Seite 216](#)).
- Filter** Mit der Definition von Filtern (siehe [Kapitel 8.2.8, Seite 338](#)) und lokalen Filtern (siehe [Kapitel 8.2.9, Seite 352](#)) können Sie unbefugten Zugriff ebenfalls verhindern.

8.2.7 NAT (Network Address Translation)

▶▶ NAT ist ein einfach zu bedienendes Verfahren, das zu drei 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.

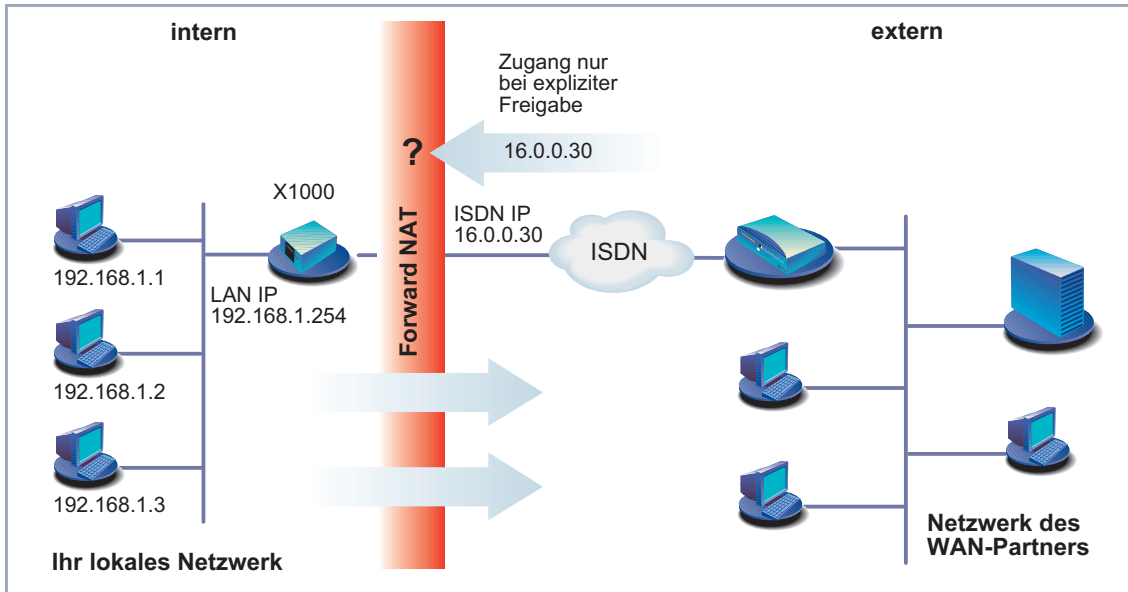


Bild 8-2: Forward NAT

■ 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. **X1000s** 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** ► **EDIT** aktivieren Sie NAT für eine Schnittstelle von **X1000**:

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 8-10: **IP** ► **NETWORK ADDRESS TRANSLATION** ► **EDIT**

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 8-11: **IP** ► **NETWORK ADDRESS TRANSLATION** ► **EDIT** ► **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.

8.2.8 Filter (Access Lists)

IP-Filter (➤➤ **Access Lists**) auf **X1000** basieren auf einem Konzept von ➤➤ **Filtern**, Regeln und sogenannten Regelketten. IP-Filter reagieren auf eingehende Datenpakete, sie können also bestimmten Daten den Zutritt zu **X1000** 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 **X1000** mit: "Achte auf diejenigen Datenpakete, auf die folgendes zutrifft: ...".

Regel Mit einer Regel teilen Sie **X1000** 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 **X1000**-Schnittstelle individuell eine Regelkette zuweisen.

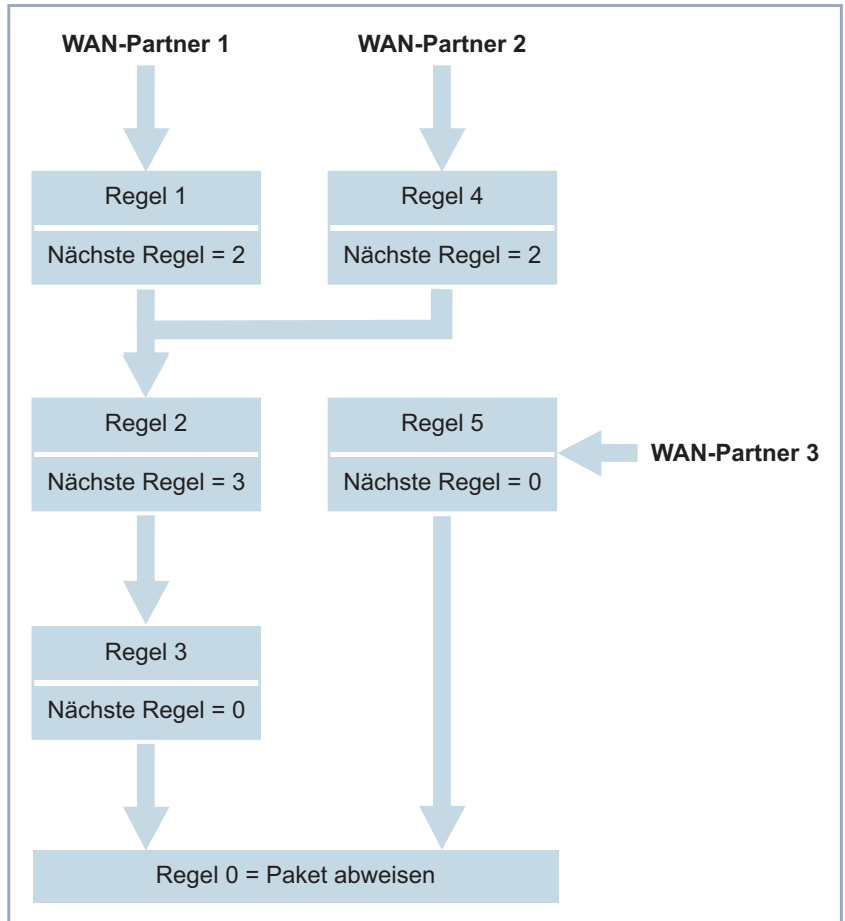


Bild 8-3: Regelketten für unterschiedliche Schnittstellen

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 angezeigt werden.
Index	Kann hier nicht verändert werden. X1000 vergibt 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.
Connection State	Bei Protocol = <i>tcp</i> können Sie ein Filter definieren, das auf dem Status der TCP-Verbindung basiert. Mögliche Werte: <i>established</i> : Das Filter paßt auf diejenigen TCP-Pakete, die beim Routing über X1000 keine neue TCP-Verbindung öffnen würden. <i>any</i> : Das Filter paßt auf alle TCP-Pakete.
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.
Source / Destination Address	Quell- bzw. Ziel-IP-Adresse der Datenpakete, auf die das Filter paßt.
Source / Destination Mask	Quell- bzw. Zielmaske. Durch die Kombination von Address und Mask wird ein Bereich von IP-Adressen beschrieben, auf den das Filter paßt.

Feld	Bedeutung
Source / Destination Port	Bereich von Port-Nummern, auf den das Filter paßt.
Specify Port	Bei Source / Destination Port = <i>specify</i> bzw. <i>specify range</i> : Port-Nummern bzw. Bereich von Port-Nummern eingeben.
Type of Service (TOS)	Type of Service
TOS Mask	Maske für Type of Service

Tabelle 8-12: 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 8-13: **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 8-14: Bereiche von Port-Nummern

Im folgenden eine Übersicht über einige häufig gebrauchte Port-Nummern mit den zugewiesenen Diensten:

Dienst	Protokoll	Port-Nummer
File Transfer Protocol (➤➤ FTP) (Daten)	TCP	20
File Transfer Protocol (FTP) (Kommandos)	TCP	21
Telnet	TCP	23
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 8-15: 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:

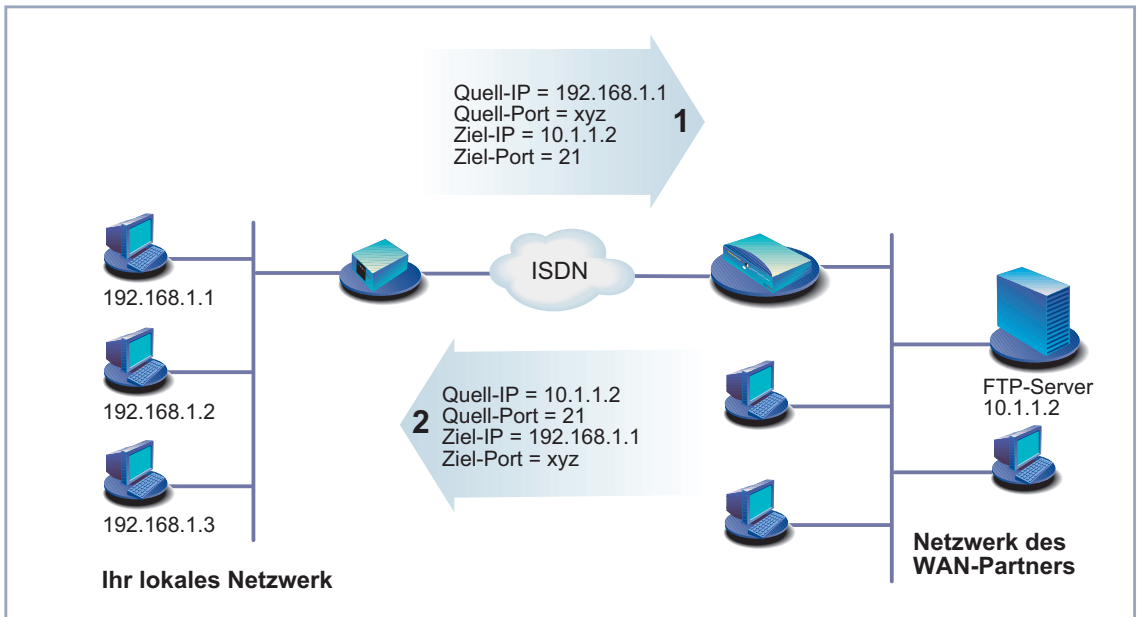


Bild 8-4: Beispiel: FTP-Verbindung

In **IP** ► **ACCESS LISTS** ► **RULES** definieren Sie Regeln:

Feld	Bedeutung
Index	Kann nicht verändert werden. X1000 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 8-16: **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 8-17: **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 8-18: **IP** ► **ACCESS LISTS** ► **RULES** ► **REORG**

Wenn Sie so eine Kette neu organisieren, nummeriert **X1000** nach Auswahl von **Index of Rule that gets Index 1** die verbleibenden Regeln neu:

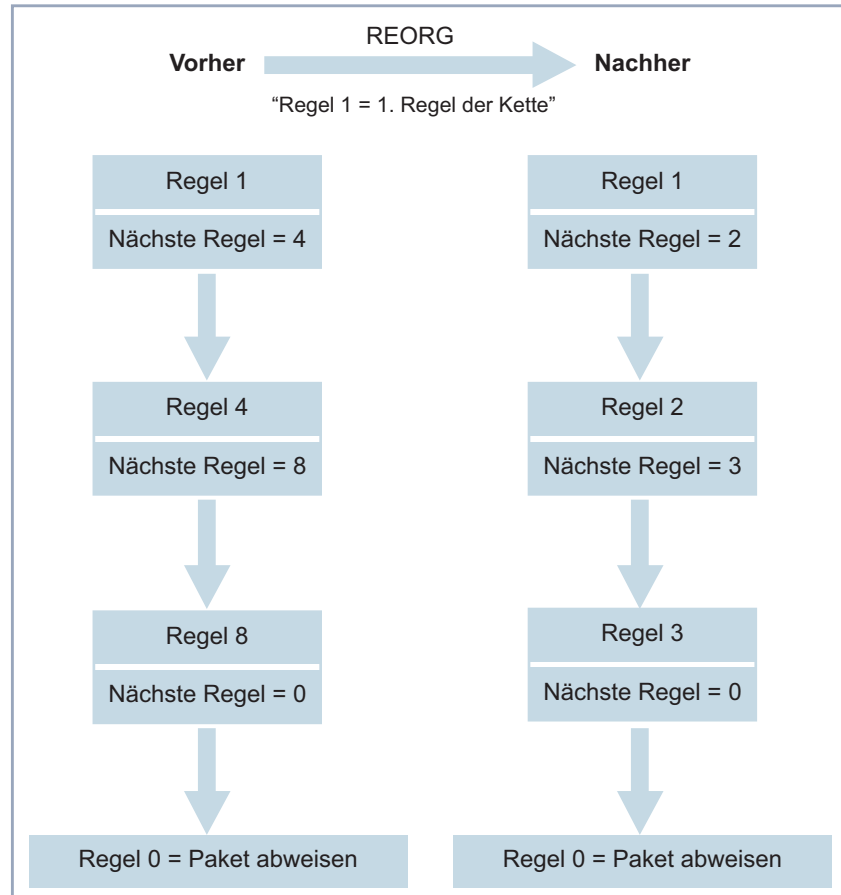


Bild 8-5: Beispiel für die Neuorganisation einer Kette

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 **X1000** 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	X1000 -Schnittstelle
First Rule	Legt fest, welche Regel als erste für Datenpakete, die über Interface X1000 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 Datenpaketes 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 8-19: 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 "aus-sperren". 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 **X1000** mit Telnet nicht mehr gestattet wird, sobald Sie die Regel eintragen und mit **SAVE** bestätigen.

- Verwenden Sie keine Filter auf dem LAN-Interface (**IP** ▶ **ACCESS LISTS** ▶ **INTERFACES** ▶ **EDIT First Rule = none**), wenn Sie aus dem LAN über Telnet auf **X1000** zugreifen.
- Wenn Sie über die serielle Schnittstelle oder ISDN-Login auf **X1000** 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**).

Regeln

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

Schnittstelle

- Verlassen Sie **IP** ➤ **ACCESS LISTS** ➤ **RULES** mit **EXIT**.
- Gehen Sie zu **IP** ➤ **ACCESS LISTS** ➤ **INTERFACES**.
- Wählen Sie eine Schnittstelle aus und bestätigen mit der **Eingabetaste**, wenn Sie eine andere als die angezeigte Regel als erste Regel für diese Schnittstelle verwenden wollen.

- Wählen Sie **First Rule** aus.
- Wählen Sie **Deny Silent** aus.
- Wählen Sie **Reporting Method** aus.
- Bestätigen Sie mit **SAVE**.

Kette neu organisieren

Gehen Sie folgendermaßen vor, um eine bestehende Kette von Regeln neu zu organisieren:

- Gehen Sie zu **IP** ➤ **ACCESS LISTS** ➤ **RULES** ➤ **REORG**.
- Wählen Sie **Index of Rule that gets Index 1** aus.
- Bestätigen Sie mit **REORG**.



Wenn Sie in Ihrem Netzwerk mit Windows-PCs arbeiten, ist es meistens sinnvoll, ein NetBIOS-Filter zu definieren. Dieses Konfigurationsbeispiel finden Sie in [Kapitel 6.1.6, Seite 162](#) Schritt für Schritt erläutert.

8.2.9 Lokale Filter

Der Zugang zu den lokalen UDP- bzw. TCP-Diensten auf **X1000** (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 8.2.7, Seite 333](#)) oder globalen Filtern (siehe [Kapitel 8.2.8, Seite 338](#)) verboten wurde.

Strategie

Sobald auf **X1000** mindestens ein Eintrag für lokale Filter besteht, werden eingehende Anfragen auf die entsprechenden lokalen Dienste von **X1000** nur erlaubt, wenn

1. die Quelladresse 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 anders zu handhaben ist als globale Filter und 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 X1000, zu dem der Zugang u. a. mit diesem Eintrag geregelt werden soll. Mögliche Werte:</p> <ul style="list-style-type: none"> ■ <i>snmp(udp)</i> ■ <i>rip (udp)</i> ■ <i>bootps(udp)</i> ■ <i>dns(udp)</i> ■ <i>telnet(tcp)</i> ■ <i>trace(tcp)</i> ■ <i>snmp(tcp)</i> ■ <i>capi(tcp)</i> ■ <i>tapi(tcp)</i> ■ <i>rfc1086(tcp)</i> ■ <i>http(tcp)</i> ■ <i>nbns(udp)</i> ■ <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"> ■ <i>verify</i> ■ <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 Quelladresse, wird zum nächsten Eintrag übergegangen.
Mask	(nur bei Verify IP Address = verify) Definiert eine Netzmaske. Zusammen mit IP Address wird damit eine Netzwerkadresse definiert, von der eingehende Anfragen auf den unter Service festgelegten Dienst erlaubt wer- den. Hat eine Anfrage eine andere Quell- adresse, wird zum nächsten Eintrag übergegangen. 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 X1000 -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 X1000 . Erreicht X1000 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 8-20: 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 **X1000** 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.

8.2.10 Backroute Verification

Hinter diesem Begriff versteckt sich eine einfache, aber sehr leistungsfähige Funktion von **X1000**. Wenn Backroute Verification bei einem WAN-Partner aktiviert ist, werden über die Schnittstelle zum WAN-Partner nur Datenpakete transportiert, die auf dem Rückweg über die gleiche Schnittstelle geroutet würden. Dadurch können Sie – auch ohne Filter – die Einspeisung von Paketen mit gefälschten IP-Adressen in Ihr LAN verhindern. Bekannte und noch unbekannte Denial of Service- und IP-Spoofing-Attacks 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**.

8.2.11 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 BinTecs Corporate Access Routern können Sie diese Funktion freischalten und den Router als TAF Server einrichten. Den Personal Access Router **X1000** können Sie als TAF ➤➤ **Client** konfigurieren und sich so auf einem TAF Server und dem angeschlossenen LAN Zugang verschaffen (wenn der TAF Server entsprechend eingerichtet wurde). Die genaue Darstellung der Funktionsweise und die erforderlichen Konfigurationsschritte finden Sie in BRICKware for Windows.

8.2.12 Extended IP-Routing (XIPR)

Ergänzend zu der normalen Routing-Tabelle kann **X1000** auch Routing-Entscheidungen aufgrund einer zusätzlichen Tabelle, der Extended-Routing-Tabelle, treffen (Erweitertes IP-Routing). Dabei kann **X1000** 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.

8.3 Abhörsicherung

Für sicherheitskritische PPP-Verbindungen können Sie einen Verschlüsselungsmechanismus einsetzen, wenn beide Verbindungspartner diesen unterstützen. Folgende Funktionen sind möglich:

- Verschlüsselung ([Kapitel 8.3.1, Seite 359](#))
- VPN (mit Zusatzlizenz, [Kapitel 8.3.2, Seite 363](#))

8.3.1 Verschlüsselung

X1000 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 und nur im Rahmen einer VPN-Lizenz verfügbar.

MPPE V2 Das Verschlüsselungsprotokoll MPPE Version 2, Nachfolger von MPPE, wurde von Microsoft entwickelt und verwendet ebenso einen 40-Bit-, 56-Bit- oder 128-Bit-Schlüssel wie Version 1.

Wenn auf **X1000** 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 **X1000** 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 **X1000** 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"> ■ <i>MPPE 40</i>: MPPE Version 1 mit 40-Bit-Schlüssel ■ <i>MPPE 56</i>: MPPE Version 1 mit 56-Bit-Schlüssel ■ <i>MPPE 128</i>: MPPE Version 1 mit 128-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>MPPE V2 128</i>: MPPE Version 2 mit 128-Bit-Schlüssel ■ <i>Blowfish 56</i>: Blowfish mit 56-Bit-Schlüssel ■ <i>Blowfish 168</i>: Blowfish mit 168-Bit-Schlüssel ■ <i>DES 56</i>: DES mit 56-Bit-Schlüssel ■ <i>DES3 168</i>: Triple DES mit 168-Bit-Schlüssel ■ <i>none</i>: keine Verschlüsselung <p>Diese Werte sind nur verfügbar, wenn unter Encapsulation <i>PPP</i>, <i>Async PPP over X.75</i>, <i>Async PPP over X.75/T.70/BTX</i> oder <i>X.25_PPP</i> ausgewählt wurde.</p>

Tabelle 8-21: **WAN PARTNER** ► **EDIT**

Bei Verwendung von DES oder Blowfish kann der Schlüssel bei der Authentisierung dynamisch 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 X1000 dynamisch 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 8-22: **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 den WAN-Partner aus, mit dem Daten verschlüsselt ausgetauscht werden sollen, und bestätigen Sie mit der **Eingabetaste**, um die 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**.

8.3.2 VPN (mit Zusatzlizenz)

Mit Hilfe von PPTP (Point to Point Tunneling Protocol) kann **X1000** ein VPN (Virtual Private Network) herstellen. Dies dient zu einer sicheren (verschlüsselt) Übertragung von Daten über WAN-Verbindungen, z. B. über das Internet. So kann z. B. von Außendienstmitarbeitern per Laptop ein Zugang auf Daten des Firmennetzes kostengünstig über das Internet realisiert werden (Einwahl über einen örtlichen Internet Service Provider).



Detaillierte Informationen und Konfigurationshinweise (mit Beispielen) finden Sie in der Software Reference.

8.3.3 IPSec (mit Zusatzlizenz)

Der Sicherheitsstandard IPSec (Internet Protocol Security) ermöglicht Ihnen, IP-basierte Daten sicher über öffentliche Netze (z. B. das Internet) auszutauschen.



Detaillierte Informationen und Konfigurationshinweise finden Sie im IPSec Reference Manual, das Sie zusammen mit Ihrer IPSec-Lizenz erhalten, bzw. in der Software Reference.

8.4 Besonderheiten

8.4.1 Startup-Verhalten

X1000 nimmt seine Routing-Tätigkeiten erst auf, wenn die komplette Konfiguration, insbesondere auch die definierten Filter, geladen sind. Somit ist es nicht möglich, durch Provokation eines Systemstarts einen Zwischenzustand des Systems auszunutzen, in dem vielleicht schon geroutet wird, aber noch keine Filter aktiv sind.

8.4.2 Autologout

Verbindungen zu **X1000** über Telnet, **ISDN-Login** oder seriell werden automatisch getrennt, wenn 15 Minuten lang keine Eingabe über die Tastatur erfolgt. Damit wird das Auslesen oder Ändern der Systemkonfiguration auf "vergessenen" Verbindungen erschwert. Den Zeitraum können Sie mit dem Kommando `t <Zeit in Sekunden>` verändern (siehe [Kapitel 12.1, Seite 410](#)).

8.4.3 Vorbeugung gegen Denial-of-Service-Angriffe

Eine Denial-of-Service-Angriffe (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-Angriffe auf den Router selbst werden bereits durch die interne Codierung unterbunden.

Z. B. existiert an allen **X1000**-Schnittstellen, für die Sie Network Address Translation (NAT) aktivieren, ein Schutz für die angeschlossenen Rechner gegen einige DoS-Angriffe mit fragmentierten Paketen. Die Paketfragmente werden beim Durchgang durch NAT wieder zusammengesetzt, bevor das Paket den Router passieren kann.

Einige DoS-Angriffe, die mit gefälschten Quell-IP-Adressen arbeiten, können Sie gegebenenfalls mit Hilfe der Funktion Backroute Verification verhindern (siehe [Kapitel 8.2.10, Seite 356](#)).

DoS-Angriffe, die auf Systemstörung durch Überlaufen von Logdateien (Syslog Messages) spekulieren, können Sie durch geeignete Platzierung und Größenlimitierung dieser Dateien begegnen.

8.5 Checkliste

Die nachfolgende Liste gibt die wichtigsten sicherheitskritischen Punkte an, die Sie bei der Konfiguration von **X1000** beachten sollten:

- Haben Sie alle vier Paßwörter für den Systemzugang (admin, read, write, http) verändert? Siehe [Kapitel 6.1.2, Seite 140](#).
- Werden die Aktivitäten von **X1000** auf mindestens einem externen Rechner ausreichend genau protokolliert und überprüfen Sie die Syslog Messages regelmäßig? Siehe [Kapitel 8.1.1, Seite 308](#).
- 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 8.2.7, Seite 333](#).
- 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 8.2.8, Seite 338](#).
- Haben Sie ggf. den Zugang über ISDN-Login für Fernwartung gesperrt? Haben Sie einen geeigneten Eintrag unter **CM-1BRI, ISDN SO ➤ INCOMING CALL ANSWERING** gemacht? Siehe [Kapitel 6.1.4, Seite 146](#).

Als zusätzliche Punkte sollten Sie beachten:

- Verwenden Sie für PPP-Verbindungen Callback nach dem Microsoft-Verfahren? Beachten Sie bitte die Hinweise in [Kapitel 8.2.4, Seite 330](#).
- Setzen Sie auf sicherheitskritischen Verbindungen ein Verschlüsselungsprotokoll zur Abhörsicherung ein? Siehe [Kapitel 8.3.1, Seite 359](#).

- Setzen Sie auf sicherheitskritischen Verbindungen eine personenbezogene Authentisierung ein?
- Erlauben Sie die Beeinflussung durch Routing-Protokolle (z. B. RIP) nur an vertrauenswürdigen Netzen? Siehe [Kapitel 7.2.8, Seite 256](#).
- Kontrollieren Sie, welche Rechner Zugang auf die Remote-CAPI-Schnittstelle haben, welche Applikationen darauf verwendet werden und ob die Verbindungen, die mit diesen Applikationen verwendet werden, erwünscht sind. Nutzen Sie das CAPI-User-Konzept?
- Sind eventuell zusätzlich angelegte Benutzer-Accounts unproblematisch?
- Haben Sie das Abhören von Verbindungen auf dem Ethernet durch eine geeignete LAN-Infrastruktur verhindert?

9 Konfigurationsmanagement

In diesem Kapitel finden Sie Hinweise zum Verwalten Ihrer Konfigurationsdateien und zum Updaten der Software von **X1000**. Es umfasst folgende Bereiche:

- Verwalten der Konfigurationsdateien:
 - Wo sind die Konfigurationsdateien?
 - Was ist Flash und Memory?
 - Wie kann ich mit Konfigurationsdateien umgehen?
- **X1000** in den Auslieferungszustand versetzen
 - Wie kann ich **X1000** in den Auslieferungszustand zurückversetzen, ohne die vorhandene Konfiguration zu löschen?
- Software Update durchführen
 - Wie bleibt mein **X1000** immer auf dem neuesten Stand?
 - Wie lade ich eine neue System-Software?

9.1 Konfigurationsdateien verwalten

Flash **X1000** liest seine Konfigurationsinformationen aus Konfigurationsdateien. Diese Konfigurationsdateien sind gespeichert im Flash EEPROM (electronically erasable programmable read-only memory) von **X1000**. Im Flash-Speicher können einige verschiedene Konfigurationsdateien gespeichert werden. Auch wenn **X1000** 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 **X1000** einstellen. Der Inhalt von Memory geht verloren, wenn **X1000** ausgeschaltet wird. Wenn Sie Ihre Konfiguration ändern und diese Änderungen auch beim nächsten Start von **X1000** beibehalten wollen, müssen Sie die geänderte Konfiguration vor dem Ausschalten im Flash speichern: **Exit** ► **Save as boot configuration and exit** (siehe [Kapitel 6.3, Seite 211](#)). Diese Datei wird damit als Boot-Konfigurationsdatei mit dem Namen "boot" im Flash gespeichert. Beim Starten von **X1000** wird dann genau diese Datei, also die Konfigurationsdatei mit dem Namen "boot", im Memory geladen und damit wirksam.

Auslieferungszustand Sollten Sie **X1000** in den Auslieferungszustand zurücksetzen und die gespeicherte Konfiguration erhalten wollen, so ist dies durch gezieltes Aus- und Einschalten des Geräts möglich (siehe [Kapitel 9.2, Seite 379](#)). Sie können **X1000** aber auch in den Auslieferungszustand versetzen und alle Konfigurationsdateien löschen (siehe [Kapitel 11.5, Seite 406](#) bzw. [Kapitel 9.2, Seite 379](#)).

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 **X1000** 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 **X1000** auf Ihrem lokalen Rechner abspeichern.



Die mit dem TFTP-Server der DIME Tools zu transferierenden Dateien dürfen maximal aus acht Zeichen bestehen (plus maximal drei Zeichen als Extension), z. B. X1000.cf.

Unix Unter Unix ist ein TFTP-Server Teil des Systems. Beachten Sie bitte die Hinweise in der Software Reference.

Mit Hilfe des Setup Tools können Sie die verschiedenen Aktionen ausführen:

➤ Gehen Sie in das Menü **CONFIGURATION MANAGEMENT**.

X1000 Setup Tool	BinTec Communications AG MyX1000
Operation	get (TFTP --> FLASH)
TFTP Server IP Address	192.168.1.1
TFTP File Name	brick.cf
Name in Flash	boot
Type of last operation	get (TFTP --> FLASH)
State of last operation	done
START OPERATION	EXIT
Use <Space> to select	

Das Menü enthält folgende Felder:

Feld	Bedeutung
Operation	Aktion, die Sie ausführen möchten.
TFTP Server IP Address	Die IP-Adresse oder der Host-Name (falls der Host-Name aufgelöst werden kann) des TFTP-Servers von bzw. zu dem Sie eine Konfigurationsdatei transferieren wollen.
TFTP File Name	Name der Konfigurationsdatei auf dem TFTP-Server (ohne Pfadangabe).
Name in Flash	Name der Konfigurationsdatei im Flash.
New Name in Flash	Name der neu zu erzeugenden Konfigurationsdatei im Flash (bei Operation = <i>move</i> oder <i>copy</i>).
Type of last operation	Vorhergehende Aktion (seit dem letzten X1000 -Start).
State of last operation	Status der letzten Aktion.

Tabelle 9-1: **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. Stellen Sie sicher, daß der TFTP-Daemon des Zielsystems Schreibrechte auf das TFTP-Verzeichnis hat.
<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 <i>load</i> (FLASH --> MEMORY) erforderlich, damit die Einstellungen auf X1000 wirksam werden.

Mögliche Werte	Bedeutung
<i>state</i> (MEMORY --> TFTP)	Alle aktuellen Einstellungen im Memory als <TFTP File Name> auf TFTP-Host mit der IP-Adresse <TFTP Server IP Address> speichern. <TFTP File Name> wird dabei überschrieben oder neu erzeugt.
<i>reboot</i>	X1000 neu starten. Einstellungen im Memory werden durch Einstellungen von boot aus Flash ersetzt.

Tabelle 9-2: **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, vgl. Kapitel 8.1.1, Seite 308).

Tabelle 9-3: **State of last operation**

Wenn beim Ausführen der Aktion *get (TFTP --> FLASH)* ein Fehler auftritt und die Aktion abgebrochen wird, ist die zu überschreibende Datei im Flash gelöscht. Wenn Sie also eine Datei "boot" transferieren, wird in diesem Fall **X1000s** Boot-Datei gelöscht, **X1000** 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. Stellen Sie sicher, daß der TFTP-Daemon des Zielsystems Schreibrechte auf das TFTP-Verzeichnis hat.

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 die 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 der Anhang (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 **X1000**

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 **X1000** transferieren wollen, gehen Sie folgendermaßen vor:

➤ Windows-PC: Klicken Sie auf **Programme** ➤ **BRICKware** ➤ **DIME Tools** im Windows-Startmenü, um **DIME Tools** zu starten. Der TFTP-Server muß aktiv sein.

➤ Aktivieren eines TFTP-Servers unter Unix: siehe Software Reference.

➤ Gehen Sie zu **CONFIGURATION MANAGEMENT**.

TFTP-Host --> Flash ➤ Wählen Sie **Operation** aus: *get (TFTP --> FLASH)*.

➤ Tragen Sie **TFTP Server IP Address** ein, z. B. *192.168.1.1*.

➤ Tragen Sie **TFTP File Name** ein: *brick.cf*.

➤ Tragen Sie **Name in Flash** ein, z. B. *boot*.

➤ Wählen Sie **START OPERATION** aus und bestätigen Sie mit der **Eingabetaste**.

Solange die Aktion ausgeführt wird, erscheint in der Hilfszeile des Setup Tools **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 **X1000** gespeichert.

Gehen Sie anschließend folgendermaßen vor, um die Einstellungen von brick.cf sofort auf **X1000** 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 Tools *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 **X1000** geladen, die Einstellungen sind aktiv.

- Verlassen Sie **CONFIGURATION MANAGEMENT** mit **EXIT**.

Sie befinden sich wieder im Hauptmenü.



Mit dem Protokoll XMODEM gibt es über die serielle Schnittstelle eine weitere Möglichkeit, Konfigurationsdateien zu transferieren. Die Vorgehensweise wird in der Software Reference dargestellt.

9.2 X1000 in den Auslieferungszustand versetzen

Durch eine spezielle Reset-Sequenz (gezieltes Ein-/Ausschalten) können Sie **X1000** in den sogenannten "Factory-Reset"-Zustand versetzen. Dieser Zustand entspricht dem einer gebooteten **X1000** im Auslieferungszustand. Sie können sich dann mit ISDN-Login (siehe [Kapitel 5.1.3, Seite 116](#)) von einem anderen Standort aus auf dem Gerät einwählen.

Im "Factory-Reset"-Zustand wird eine existierende Boot-Konfiguration ignoriert aber nicht gelöscht, die Default-Konfiguration wird verwendet.

Um **X1000** in den "Factory-Reset"-Zustand zu versetzen, gehen Sie folgendermaßen vor:

- Schalten Sie **X1000** aus, wenn das Gerät vorher in Betrieb war.
- Schalten Sie **X1000** ein, damit das Gerät die Boot-Sequenz durchläuft (siehe [Kapitel 11.5, Seite 406](#)).
- Beobachten Sie die LEDs auf der Vorderseite von **X1000**. Nach Durchlaufen des Startmodus (ca. 8 Sekunden; siehe [Kapitel 11.2, Seite 399](#)) leuchten alle gelben LEDs gleichzeitig. (Wenn **X1000** über die serielle Schnittstelle mit Ihrem Rechner verbunden ist und **HyperTerminal** gestartet ist (siehe [Kapitel 5.1.1, Seite 113](#)), erscheint zu diesem Zeitpunkt auf dem Bildschirm die Meldung `Press <sp>.`)
- Schalten Sie das Gerät aus während die gelben LEDs leuchten. Sie haben dazu etwa 4 Sekunden Zeit.
- Wiederholen Sie den Ein-/Ausschaltvorgang zweimal. Insgesamt wurde **X1000** dreimal ein- und ausgeschaltet.
- Schalten Sie **X1000** zum vierten Mal ein. Wenn Sie die Boot-Sequenz diesmal nicht unterbrechen, so läuft das Gerät im "Factory-Reset"-Zustand hoch. Dreimaliges Blinken aller gelben LEDs signalisiert Ihnen diesen Zustand.

Um **X1000** im "Factory-Reset"-Zustand vor unberechtigtem Zugriff zu schützen, benötigen Sie zum Einwählen das Paßwort der zuvor aktiven Boot-Konfiguration.

Sie können sich mit ISDN-Login und diesem Paßwort einloggen, um z. B. die Boot-Konfiguration zu laden, zu modifizieren und abzuspeichern.

Optional können Sie beim Login-Prompt `erase bootconfig` eingeben. Dieser Befehl löscht alle bestehenden Konfigurationen, **X1000** wird neu gebootet.

Wenn Sie das Gerät ein weiteres Mal aus- und wieder einschalten, läuft es mit der gespeicherten Boot-Konfiguration hoch.

9.3 Software Update durchführen

Da BinTec Communications AG die Software für alle Produkte ständig weiterentwickelt und Sie sicher die neuesten Funktionen von **X1000** nutzen wollen, erfahren Sie hier, wie Sie ein Software Update durchführen können.

www.bintec.de Wenn Sie ein Software Update durchführen, spielen Sie auf **X1000** eine neue System-Software ein. Jede System-Software beinhaltet neue Funktionen, bessere Performance und bei Bedarf Bugfixes der vorhergehenden Version. Die aktuelle von BinTec Communications AG zur Verfügung gestellte System-Software (Boot-Image) 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, BRICKware for Windows).



Wenn Sie ein Software Update durchführen, beachten Sie unbedingt die dazugehörige Release Note. Hier sind die Änderungen beschrieben, die mit der neuen System-Software zur Verfügung stehen.

update Es gibt verschiedene Möglichkeiten, ein Software Update durchzuführen. In diesem Kapitel erfolgt das Update mit Hilfe des update-Kommandos auf der SNMP-Shell und wird Schritt für Schritt genau beschrieben. Weitere Möglichkeiten finden Sie in der Software Reference und in [Kapitel 11.5, Seite 406](#).



In seltenen Fällen ist zusätzlich ein Update von Bootmonitor und/oder Firmware Logic empfohlen. Falls dies bei einem neuen Release nötig sein sollte, ist dies ausdrücklich in der entsprechenden Release Note vermerkt. Die Vorgehensweise und Empfehlung finden Sie in der Release Note BOOTmonitor and Firmware Logic Update.

Soweit BinTec Communications AG keine explizite Empfehlung ausspricht, BOOTmonitor oder Firmware Logic upzudaten, sollten Sie dies nicht tun!

ToDo Gehen Sie folgendermaßen vor, um ein Software Update (Boot-Image) durchzuführen:



Schalten Sie **X1000** nicht aus, während das Update durchgeführt wird!

- Geben Sie die ➤➤ **URL** www.bintec.de in Ihren Browser (z. B. Internet Explorer oder Netscape Navigator) ein.
Die BinTec-Homepage erscheint. Unter der entsprechenden Rubrik finden Sie die aktuelle Software und Dokumentation für **X1000**.
- Klicken Sie mit der rechten Maustaste auf die aktuelle System-Software (Boot-Image, Software-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 die neue System-Software auf Ihrem Rechner gespeichert werden soll. Als Verzeichnis dient normalerweise C:\BRICK bei Windows-PCs und /tftpboot bei Unix-Workstations. Als Name können Sie z. B. **b5104b02.x1x** übernehmen.
- Bestätigen Sie mit **SAVE**.
Die System-Software wird auf Ihrem Rechner abgespeichert.
- Aktivieren Sie einen TFTP-Server auf Ihrem Rechner.
Windows-PC: Klicken Sie auf **Programme** ➤ **BRICKware** ➤ **DIME Tools** im Windows-Startmenü, um die **DIME Tools** zu starten (Installation der **DIME Tools**, siehe Kap. [Kapitel 3.3, Seite 47](#)). Aktivieren Sie den TFTP-Server.
Unix-Rechner: Beachten Sie die Hinweise in der Software Reference.
- Loggen Sie sich auf **X1000** 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. Die spitzen Klammern fallen bei der Eingabe weg.
<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 die neue System-Software abgespeichert haben (z. B. 192.168.1.1).

<Dateiname> ist der Name der System-Software, die Sie auf Ihrem Rechner abgespeichert haben (z. B. **b5104b02.x1x**).

Die Datei <Dateiname> wird zunächst in den Arbeitsspeicher von **X1000** 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, die neue System-Software wird in den Flash-Speicher geladen.



X1000 benötigt einen zusammenhängenden Block an freiem Arbeitsspeicher, der etwas größer als die neue System-Software ist. Wenn auf **X1000** nicht genügend Arbeitsspeicher zu Verfügung steht, bietet **X1000** ein sogenanntes "incremental update" an, wobei die Software "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**.

X1000 führt ein incremental update aus, die Software 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**.

X1000 startet mit der neuen System-Software. Die vorhandene Konfiguration wird übernommen.

10 Trouble Shooting

Tips Wenn Sie Probleme mit **X1000** haben, helfen Ihnen die folgenden Tips häufig schon weiter:

- Loggen Sie sich auf **X1000** 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 **X1000** erzeugten Syslog Messages (siehe [Kapitel 8.1.1, Seite 308](#)). 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 Trouble Shooting
- Typische Fehlersituationen

10.1 Hilfsmittel zum Trouble Shooting

Hier finden Sie Methoden, um die Ursache Ihres Problems einzugrenzen:

- Lokale SNMP-Shell-Kommandos
- Externe Hilfsmittel

10.1.1 Lokale SNMP-Shell-Kommandos

Diese Kommandos geben Sie direkt in die SNMP-Shell von **X1000** ein:

debug

Mit dem Kommando `debug` können Sie die Fehlersuche für eines oder mehrere Subsysteme von **X1000** betreiben. Eine genaue Erläuterung der Syntax und der Optionen finden Sie in [Kapitel 12.1, Seite 410](#).

Beispiele:

- Geben Sie `debug all` ein, um Debugging-Informationen für alle Subsysteme anzuzeigen.
- Geben Sie `debug config &` ein, um Problemen beim Konfigurationsmanagement auf die Spur zu kommen (siehe [Kapitel 9, Seite 369](#)).



Wenn Sie einem SNMP-Shell-Kommando ein `&` anhängen, wird das Programm im Hintergrund ausgeführt.

isdnlogin

Mit dem Kommando `isdnlogin` können Sie überprüfen, ob eine ISDN-Verbindung zustande kommen kann. Eine Beschreibung finden Sie in [Kapitel 12.1, Seite 410](#).

Beispiel:

- Geben Sie `isdnlogin 1234 telephony` ein, um ein Telefon mit der Rufnummer 1234 in Ihrem lokalen Büro anzurufen.
Wenn eine Verbindung zustandekommt, klingelt das Telefon.

trace

Mit dem Kommando `trace` können Sie über ISDN (D- und B-Kanäle) oder über das LAN gesendete und empfangene Datenpakete anzeigen und interpretieren lassen. Eine Beschreibung der Syntax finden Sie in [Kapitel 12.1, Seite 410](#).

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 **X1000s** MAC-Adresse über das LAN zum Host mit der MAC-Adresse 0:a0:f9:d:5:a verschickt werden.

10.1.2 Externe Hilfsmittel

Mit den folgenden Hilfsprogrammen können Sie von einem Windows-PC oder einem Unix-Rechner aus Verbindungen mit **X1000** analysieren.

DIME Tracer (Windows)

Der DIME Tracer ermöglicht, **X1000s** 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 **X1000s** ISDN-Kanäle laufende Daten von einem Unix-Rechner aus zu überprüfen. `bricktrace` ist Teil der BRICKtools für UNIX auf Ihrer BinTec Companion CD. Eine ausführliche Beschreibung finden Sie in [Kapitel 12.2, Seite 417](#).

10.2 Typische Fehlersituationen

Im folgenden finden Sie eine Zusammenstellung typischer Fehlersituationen und Hinweise zu Diagnose und "Heilung". Versuchen Sie, das auftretende Problem einzugrenzen. Folgende Kategorien stehen zur Verfügung:

- Systemfehler
- ISDN-Verbindungen
- IPX-Routing

10.2.1 Systemfehler

Ich habe mein Paßwort vergessen.

Sie müssen **X1000** in den unkonfigurierten Anfangszustand (Auslieferungszustand) zurückversetzen:

- Verbinden Sie Ihren Rechner über die serielle Schnittstelle mit **X1000** wie in [Kapitel 5.1.3, Seite 116](#) beschrieben.
- Schalten Sie **X1000** 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 **X1000** werden gelöscht.
- Wählen Sie (1) Boot System.
X1000 wird neu gestartet.
- Konfigurieren Sie **X1000** erneut.

Ich kann X1000 im LAN nicht erreichen.

Versuchen Sie eine serielle Verbindung herzustellen:

- Verbinden Sie Ihren Rechner über die serielle Schnittstelle mit **X1000**.
- Loggen Sie sich als Benutzer `admin` mit dem entsprechenden Paßwort ein.
- Starten Sie das Setup-Tool mit `setup`.
- Untersuchen Sie, ob ein Konfigurationsfehler die Ursache ist:
Haben Sie unter **CM-100BT, FAST ETHERNET** die IP-Adresse eingetragen?
Haben Sie unter **IP** ➤ **ACCESS LISTS** ein Filter eingetragen, das Sie aussperrt?
Haben Sie unter **IP** ➤ **NETWORK ADDRESS TRANSLATION** ➤ **EDIT** für eine Ethernet Schnittstelle (en1 bzw. en1-snap) NAT aktiviert und vergessen, für diese Schnittstelle unter **IP** ➤ **NETWORK ADDRESS TRANSLATION** ➤ **EDIT** ➤ **ADD** die gewünschten IP-Verbindungen zu erlauben.
Machen Sie die erforderlichen Korrekturen.

Wenn auch eine serielle Verbindung nicht klappt:

- Überprüfen Sie die Einstellungen des Terminal-Programms (siehe [Kapitel 5.1.1, Seite 113](#)). Wenn Sie die Standardeinstellungen im BOOTmonitor verändert haben, passen Sie Ihre Terminal-Einstellungen daran an.
- Wenn Sie keinen Erfolg haben, gehen Sie vor wie unter "Ich habe mein Paßwort vergessen" beschrieben.

10.2.2 ISDN-Verbindungen

Hier finden Sie mögliche Fehlerquellen für ISDN-Verbindungen.

Die Telefonrechnung ist ungewöhnlich hoch.



Nutzen Sie die Funktion Taschengeldkonto (siehe [Kapitel 8.1.3, Seite 317](#)). Damit können Sie für Verbindungen mit **X1000** ein Limit festlegen, um Gebühren aufgrund von Fehlern bei der Konfiguration in Grenzen zu halten.

Möglicherweise gibt es auf **X1000** ISDN-Verbindungen, die ständig offen bleiben oder es werden ungewollte ISDN-Verbindungen provoziert.

- Überprüfen Sie mit `debug all` oder `trace`, ob ein Rechner im LAN eine andere Netzmaske verwendet als auf **X1000** 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 **X1000** so konfiguriert ist, daß Syslog-Messages auf einen Host außerhalb des LANs geschickt werden (Zielport 514).
- Überprüfen Sie in der MIB-Tabelle **biboAdmTrapHostTable**, ob **X1000** so konfiguriert ist, daß SNMP Traps (Meldungen) auf einen Host außerhalb des LANs geschickt werden (Zielports 161, 162).
- Überprüfen Sie, ob bei Verbindungen mit dynamischem Channel Bundling häufiges Auf- und Abbauen des zweiten B-Kanals aufgrund von schwankendem Traffic geschieht.
- Überprüfen Sie mit `debug all` oder `trace`, ob ein Rechner im LAN mit einer falschen IP-Adresse für den WINS Server konfiguriert ist (Zielports 137-139). Konfigurieren Sie gegebenenfalls den Rechner richtig oder setzen Sie entsprechende Filter ein.
- Überprüfen Sie mit `debug all` oder `trace`, ob ein Rechner im LAN für Namensauflösung von NetBIOS-Namen mit Hilfe von DNS konfiguriert ist (es wird von einem Clientport aus auf Zielport 53 zugegriffen). Versuchen Sie nicht, NetBIOS-Namen mit DNS aufzulösen!
- Überprüfen Sie mit `debug all` oder `trace`, ob eine Applikation auf einem Rechner im LAN versucht, Adressen aufzulösen, die der Name-Server beim Internet Service Provider nicht kennt (es wird von einem Clientport aus auf Zielport 53 zugegriffen). Richten Sie eine lokale HOSTS-Datei im Windows-Verzeichnis ein, die die Namensauflösung durchführen kann (siehe [Kapitel 4.5, Seite 101](#)).
- Überprüfen Sie mit `debug all` oder `trace`, ob auf einem Rechner im LAN NetBIOS over IP eingerichtet ist (es wird vom Source Port 137 auf den Zielport 53 zugegriffen). Dabei wird versucht, NetBios-Namen über DNS aufzulösen. Schalten Sie NetBIOS over IP ab oder setzen Sie Filter ein. (Die Konfiguration der entsprechenden Filter finden Sie in [Kapitel 6.1.6](#),

Seite 162. Sie können auch den einfachen NetBIOS-Filter des Configuration Wizards nutzen, siehe [Kapitel 4.7, Seite 107](#)).

- Überprüfen Sie, ob Sie Callback konfiguriert haben (siehe [Kapitel 8.2.4, Seite 330](#)) und dabei eine falsche Rufnummer eingegeben haben (**Number** unter **WAN PARTNER** ➤ **EDIT** ➤ **WAN NUMBERS** ➤ **EDIT**).
- Überprüfen Sie, ob Sie ein trace-Programm über eine ISDN-PPP-Verbindung laufen lassen. Damit werden ständig Pakete über die ISDN-Verbindung gesendet, die Verbindung bleibt permanent offen.

Ausgehende Rufe kommen nicht zustande.

- Überprüfen Sie anhand der LEDs auf der **X1000**-Vorderseite (siehe [Kapitel 11.2, Seite 399](#)), ob eine Verbindung zustande kommt.
- Überprüfen Sie mit `isdnlogin`, ob ausgehende Rufe möglich sind.
- Überprüfen Sie in **MONITORING AND DEBUGGING** ➤ **ISDN MONITOR**, ob überhaupt ein ausgehender Ruf protokolliert wurde, ob die gewählte Nummer korrekt ist und ob der Ruf verbunden war.
- Überprüfen Sie, ob ISDN-Syslog Messages mit "disconnect cause" protokolliert wurden.
- Überprüfen Sie, ob **Encapsulation** in **WAN PARTNER** ➤ **EDIT** für die Verbindungspartner identisch ist.
- Überprüfen Sie, ob **Authentication** in **WAN PARTNER** ➤ **EDIT** ➤ **PPP** für die Verbindungspartner identisch ist.
- Überprüfen Sie mit `trace`, was über die ISDN-Kanäle gesendet wird.
- Überprüfen Sie, ob die MIB-Variable **Status** in der MIB-Tabelle **isdnStkTable** den Wert *loaded* hat.
- Überprüfen Sie, ob in **CM-1BRI, ISDN SO** ➤ **INCOMING CALL ANSWERING** die eigene Rufnummer richtig eingetragen ist. Sie gilt auch für ausgehende Rufe!

Eingehende Rufe kommen nicht zustande.

- Überprüfen Sie anhand der LEDs auf der **X1000**-Vorderseite (siehe [Kapitel 11.2, Seite 399](#)), ob ein eingehender Ruf überhaupt empfangen wird.

- Überprüfen Sie in **MONITORING AND DEBUGGING** ➤ **ISDN MONITOR**, ob überhaupt ein eingehender Ruf protokolliert wurde.
- Überprüfen Sie in **WAN PARTNER** ➤ **EDIT** ➤ **WAN NUMBERS**, ob eine passende Nummer für eingehende Rufe eingetragen ist.
- Überprüfen Sie die MIB-Variablen **DSS1Cause** und **LocalCause** in der MIB-Tabelle **isdnCallHistoryTable**. Zur Interpretation der Einträge siehe Software Reference.
- Überprüfen Sie in **CM-1BRI, ISDN S0** ➤ **INCOMING CALL ANSWERING**, ob Sie für eingehende Rufe die erforderlichen Eintragungen gemacht haben.
- Überprüfen Sie, ob **Encapsulation** in **WAN PARTNER** ➤ **EDIT** für die Verbindungspartner identisch ist.
- Überprüfen Sie, ob **Authentication** in **WAN PARTNER** ➤ **EDIT** ➤ **PPP** für die Verbindungspartner identisch ist.

10.2.3 IPX-Routing

Hier finden Sie einige Probleme mit dazugehörigen Lösungsvorschlägen, die bei IPX-Routing auftreten könnten.

Überprüfen Sie mit dem Setup Tool:

- Haben Sie unter **LICENSES** die richtige Lizenz eingetragen?
- Ist in **IPX** der Eintrag unter **Internal Network Number** eindeutig im LAN?

Ein Server existiert in einem Remote LAN (LAN-LAN-Kopplung über ISDN), aber ist für Clients im lokalen LAN "unsichtbar".

Der Server könnte für Clients unsichtbar sein, weil SAP-Pakete vom Server nicht empfangen werden:

- Überprüfen Sie die Eintragungen von **Update Time** und **Age Multiplier** in **WAN PARTNER** ➤ **EDIT** ➤ **IPX**. Die Einstellungen müssen zu den Einstellungen auf den Servern im **X1000**-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 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 Netzlaufwerk des Clients wechseln.

- Möglicherweise ist der Server für den Client unsichtbar. Gehen Sie vor wie unter "Ein Server existiert in einem Remote LAN ..." beschrieben.
- Überprüfen Sie, ob die auf dem Server zur Verfügung stehenden Lizenzen alle belegt sind.

ISDN-Verbindungen werden ständig neu aufgebaut.

Es sind nicht nur RIP/SAP-Pakete, die den Aufbau von ISDN-Verbindungen verursachen.

- Überprüfen Sie, ob sich ein Eintrag in der MIB-Tabelle **ipxDenyTable** befindet, der verhindert, daß Novell Serialization-Pakete über die Wählverbindung gesendet werden.

- Überprüfen Sie, ob Sie unter **IPX enable IPX spoofing** und **enable SPX spoofing** mit *yes* aktiviert haben.
- Überprüfen Sie, ob irgendwo RCONSOLE mit einem ständig sich verändernden Bildschirm (z. B. MONITOR, IPXCON, TCPCON, ein 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 Synchronization aktiv ist (ab Netware 4.1 Server).
- Werten Sie die Syslog Messages (**Level** = *debug*) aus und filtern Sie gegebenenfalls die IPX-Pakete aus, die dort als Ursache für ungewollte Verbindungsaufbauten genannt werden.

Die MIB-Variable **ipxAdmSpxConns** enthält mehr Verbindungen als tatsächlich aktiv sind.

X1000 empfängt möglicherweise keine SPX-Abbruchmeldungen vom Server:

- Geben Sie das Kommando `reset router` an der Konsole des entsprechenden Servers ein.
Alle inaktiven Verbindungen zwischen dem Server und **X1000** werden abgebaut.
- Bei fehlender Abmeldung könnten SPX-Verbindungen noch bis zu einem Timeout bestehen und dadurch in **ipxAdmSpxConns** mitgezählt werden.

11 Technische Daten

In diesem Kapitel werden die technischen Daten von **X1000** vorgestellt. Folgende Bereiche werden behandelt:

- Allgemeine Produktmerkmale
- **X1000**-Vorderseite mit den Anzeigen (LEDs)
- **X1000**-Rückseite mit den Anschlüssen
- Pin-Zuordnung
- BOOTmonitor

11.1 Allgemeine Produktmerkmale

Die allgemeinen Produktmerkmale umfassen die Leistungsmerkmale von **X1000** und technische Voraussetzungen für Installation und Betrieb.

Bezeichnung	Werte
Produktname:	X1000
Maße und Gewichte (B x H x T): Gerätemaße ohne Kabel Aufstellgröße und Wartungsfläche Gewicht Transportgewicht (inkl. Dokumentation, Kabel, Verpackung)	141 mm x 50 mm x 145 mm 150 mm x 60 mm x 210 mm 420 g ca. 2 kg
Speicher:	8 MB DRAM, 2 MB Flash-ROM
LEDs:	5 (1 Power, 3 Funktion, 1 Error)
Leistungsaufnahme Gerät:	3 W (typisch)
Spannungsversorgung:	AC/DC-Adapter Eingang: 230V~50Hz / 70mA Ausgang: 5V-800mA 4VA
Umweltanforderungen: Lagertemperatur Betriebstemperatur Relative Luftfeuchtigkeit Raumklassifizierung	-20 bis +85°C 0 bis 50°C 20 bis 90% nichtkondensierend im Betrieb. 5 bis 95% nichtkondensierend bei Lagerung. Nur in trockenen Räumen betreiben.
MTBF-Wert:	100 000 Stunden

Bezeichnung	Werte
Verfügbare Interfaces: Serielle Schnittstelle V.24 Ethernet IEEE 802.3 LAN ISDN-WAN S ₀	Fest eingebaut, unterstützt die Baudraten: 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200 Baud. Fest eingebaut (nur twisted-pair), 10/100 MBit/s, autosensing. Fest eingebaut.
Verwendete Stecker: serielle Schnittstelle Ethernet-Schnittstelle ISDN-Schnittstelle	8-polig MiniDin RJ45 RJ45
Applikations-Schnittstelle:	Dual Remote CAPI (v1.1 und 2.0), R-CAPI-Treiber für Windows 95/98/2000/NT und Novell Netware. Source Code Library für andere Systeme (z. B. Unix, AS400).
Datenkompression:	PPP LZS STAC Kompressionsrate bis 4:1.
SAFERNET™ Security Technologie:	Community Paßworte, PAP, CHAP, MS-CHAP, Callback, Access Control Lists, Allow Lists, CLID, NAT, TAF, MPPE Encryption.
Erforderliche Lizenzen:	Lizenzen für CAPI, IP, IPX, STAC im Lieferumfang enthalten. Zusatzlizenzen für VPN, IPSec und Festverbindungen erhältlich.
Mitgelieferte Software:	RVS-COM Lite (Kommunikationsanwendung) BRICKware for Windows BRICKtools for Unix

Bezeichnung	Werte
Mitgelieferte gedruckte Dokumentation:	Benutzerhandbuch Kurzanleitung
Online-Dokumentation:	BRICKware for Windows (engl.) Software Reference (engl.) User's Guide

11.2 LEDs auf der Vorderseite

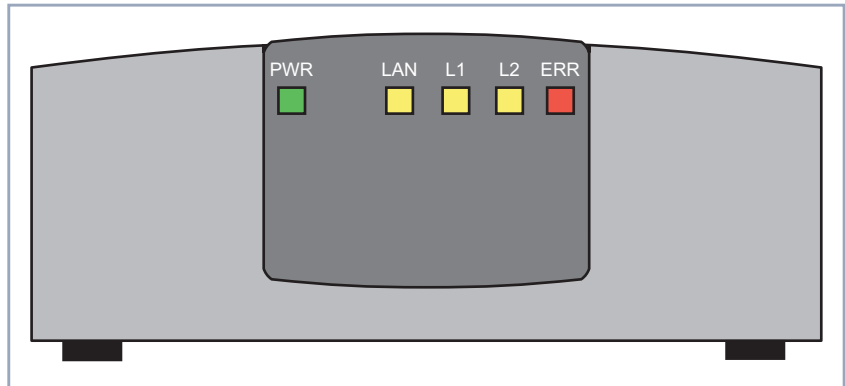


Bild 11-1: **X1000** Vorderseite

Auf der Vorderseite befinden sich fünf Anzeigen (LEDs), die Statusinformationen von **X1000** anzeigen. Jede der LEDs ist mit mehreren Bedeutungen belegt, je nachdem in welchem Modus **X1000** sich befindet. Um sicherzustellen, daß alle LEDs funktionsfähig sind, leuchten sie nach dem Einschalten des Geräts eine halbe Sekunde lang. Wenn **X1000** hochfährt, wechseln die verschiedenen Funktionszustände zwischen:

- Startmodus
- BOOTmonitor-Modus (siehe [Kapitel 11.5, Seite 406](#))
- Normaler Betriebsmodus

Die Bedeutungen der LEDs im jeweiligen Zustand sind in den folgenden Tabellen beschrieben.

Startmodus

LED	Status	Bedeutung
PWR	An	Stromversorgung ist angeschlossen.
LAN	An	LAN-(100BT)-Test wird durchgeführt.
L1	An	ISDN-Test wird durchgeführt.

LED	Status	Bedeutung
L2	An	Speicher-Test wird durchgeführt.
ERR	An	Während eines Tests ist ein Fehler aufgetreten.

Solange ein Test durchgeführt wird, leuchtet die entsprechende Funktions-LED. Ist der Test abgeschlossen, erlischt die LED. Tritt während eines Tests ein Fehler auf, so leuchtet die Error LED zusammen mit der entsprechenden Funktions-LED.

BOOTmonitor-Modus

LED	Status	Bedeutung
PWR	An	Stromversorgung ist angeschlossen.
LAN, L1, L2	An	Durch dreimaliges Aus- und Einschalten von X1000 kann das Gerät in den Auslieferungszustand versetzt werden.
LAN	Blinkend	TFTP-Transfer wird durchgeführt.
L1, L2	An	BOOTmonitor ist aktiv (oder erwartet eine Eingabe über die Tastatur).
L1, L2	Blinkend	BOOTmonitor dekomprimiert System-Software.
ERR	An	Während des Boot-Vorgangs ist ein Fehler aufgetreten, X1000 kann deshalb nicht booten.

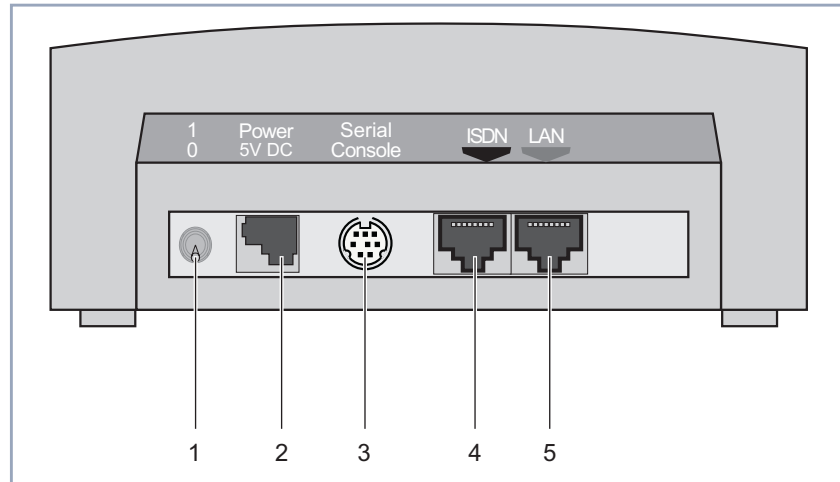
Normaler Betriebsmodus

LED	Status	Bedeutung
PWR	An	Stromversorgung ist angeschlossen.
LAN, L1, L2	Blinkend (dreimal)	Rücksetzen von X1000 in den Auslieferungszustand war erfolgreich.
LAN	An	Datenpaket passiert die LAN-Schnittstelle.
L1	Blinkend	ISDN-B1-Kanal: Verbindung wird aufgebaut.

LED	Status	Bedeutung
L1	An	ISDN-B1-Kanal Verbindung ist aktiv. (1)
L2	Blinkend	ISDN-B2-Kanal: Verbindung wird aufgebaut.
L2	An	ISDN-B2-Kanal Verbindung ist aktiv. (1)
ERR	An (zeitweilig)	LAN-Fehler oder -Kollision ist aufgetreten.
ERR	An (konstant)	System wird angehalten, Neustart ist nötig.

(1) Gebühren fallen an.

11.3 Anschlüsse auf der Rückseite



1	Ein-/Ausschalter	4	ISDN-S ₀ -Schnittstelle
2	Stromversorgungsanschluß	5	LAN-Schnittstelle (10/100 Base-T Ethernet), am Gerät rot gekennzeichnet
3	Serielle Schnittstelle		

Bild 11-2: **X1000** Rückseite

Die **X1000**-Hauptplatine enthält eine Ethernet- und eine ISDN-Schnittstelle. Diese Schnittstellen sind über die an der Rückseite angebrachten Anschlüsse ([Kapitel 11.4, Seite 403](#)) zu erreichen.



Achtung!

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

- Verwenden Sie ausschließlich das mitgelieferte Steckernetzteil (5 V DC).
- Vergewissern Sie sich, daß die auf dem Steckernetzteil vermerkte Nennspannung mit der lokalen Spannungsversorgung übereinstimmt.

11.4 Pin-Zuordnung

Serielle Schnittstelle:

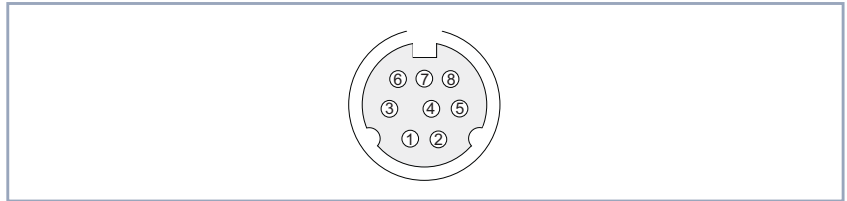


Bild 11-3: 8-polige MiniDin-Buchse

Als Konsolenanschluß stellt **X1000** eine serielle Schnittstelle mit 8-poliger MiniDin-Buchse zur Verfügung. Baudraten zwischen 1200 und 115200 werden unterstützt.

Die Pin-Zuordnung für die 8-polige MiniDin-Buchse ist wie folgt:

Pin	Funktion
1	Für zukünftige Anwendungen.
2	Für zukünftige Anwendungen.
3	T
4	GND
5	R
6	NC
7	NC
8	NC

ISDN-S₀-Schnittstelle

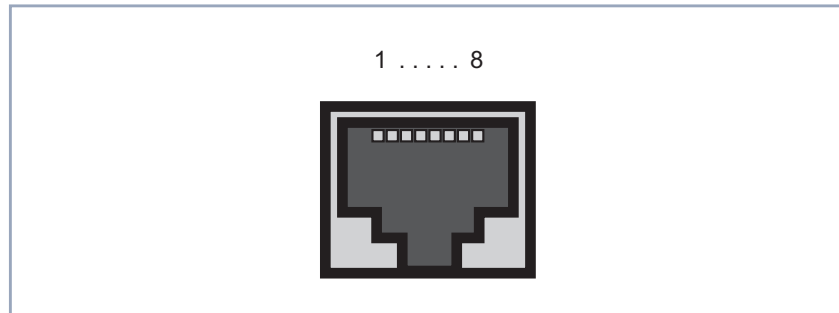


Bild 11-4: ISDN-S₀-BRI-Schnittstelle (RJ45-Buchse)

Die Pin-Zuordnung für die ISDN-S₀-BRI-Schnittstelle (RJ45-Buchse) (4) ist wie folgt:

Pin	Funktion
1	Nicht genutzt
2	Nicht genutzt
3	Senden (+)
4	Empfangen (+)
5	Empfangen (-)
6	Senden (-)
7	Nicht genutzt
8	Nicht genutzt

LAN-Schnittstelle

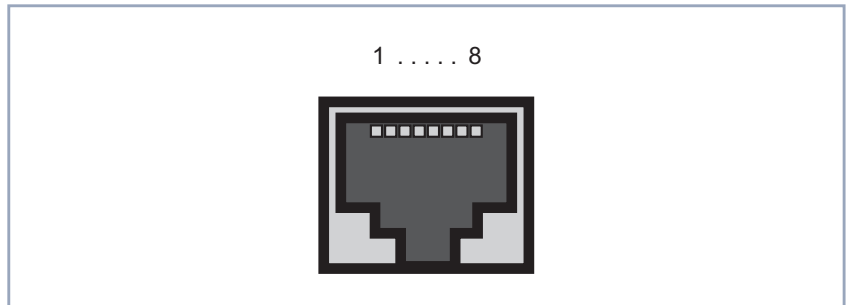


Bild 11-5: Ethernet-10/100Base-T-Schnittstelle (RJ45-Buchse)

Die Pin-Zuordnung für die Ethernet 10/100Base-T-Schnittstelle (RJ45-Buchse) ist wie folgt:

Pin	Funktion
1	TD +
2	TD -
3	RD +
4	Nicht genutzt
5	Nicht genutzt
6	RD -
7	Nicht genutzt
8	Nicht genutzt



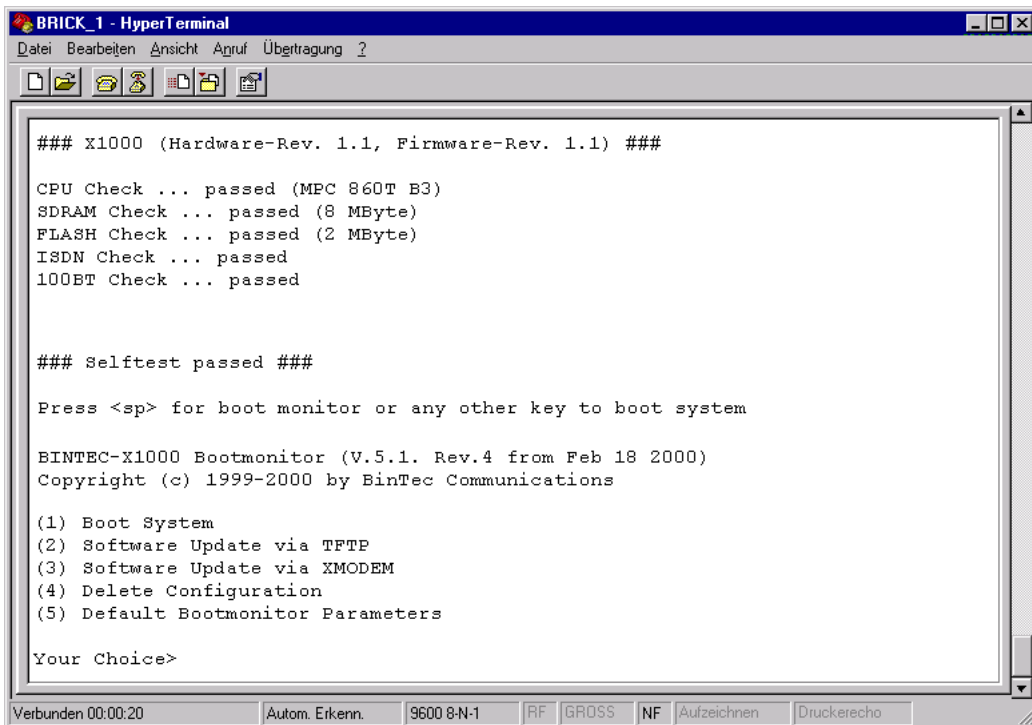
Wenn Sie die LAN-Schnittstelle von **X1000** nicht an einen externen Hub, sondern direkt an der Ethernet-Karte Ihres Rechners anschließen wollen, brauchen Sie zusätzlich zum roten LAN-Kabel das Adapter-Kabel.

11.5 BOOT-Sequenz

Beim Hochfahren von **X1000** werden verschiedene Funktionszustände durchlaufen (siehe auch [Kapitel 11.2, Seite 399](#)):

- Startmodus
- BOOTmonitor-Modus
- Normaler Betriebsmodus

Nachdem im Startmodus einige Selbsttests erfolgreich ausgeführt wurden, erreicht **X1000** den BOOTmonitor-Modus. Der BOOTmonitor-Prompt wird angezeigt, falls Sie über ein Terminal-Programm mit **X1000** verbunden sind.



```
BRICK_1 - HyperTerminal
Datei Bearbeiten Ansicht Anruf Übertragung ?

### X1000 (Hardware-Rev. 1.1, Firmware-Rev. 1.1) ###

CPU Check ... passed (MPC 860T B3)
SDRAM Check ... passed (8 MByte)
FLASH Check ... passed (2 MByte)
ISDN Check ... passed
100BT Check ... passed

### Selftest passed ###

Press <sp> for boot monitor or any other key to boot system

BINTEC-X1000 Bootmonitor (V.5.1. Rev.4 from Feb 18 2000)
Copyright (c) 1999-2000 by BinTec Communications

(1) Boot System
(2) Software Update via TFTP
(3) Software Update via XMODEM
(4) Delete Configuration
(5) Default Bootmonitor Parameters

Your Choice>
```

Bild 11-6: BOOTmonitor

BOOTmonitor Betätigen Sie nach Anzeige des BOOTmonitor-Prompts ([Bild 11-6, Seite 406](#)) innerhalb von 4 Sekunden die **Leertaste**, um die Funktionen des BOOTmonitors zu nutzen. Wenn Sie keine Eingabe machen, wechselt **X1000** nach Ablauf der 4 Sekunden in den normalen Betriebsmodus.

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:
X1000 lädt die komprimierte Boot-Datei vom Flash-Speicher in den Arbeitsspeicher. Dies wird beim Hochfahren automatisch ausgeführt.
- (2) Software Update via TFTP:
X1000 führt ein Software Update über einen TFTP-Server aus.
- (3) Software Update via XMODEM:
X1000 führt ein Software Update über eine serielle Schnittstelle mit XMODEM aus.
- (4) Delete Configuration:
X1000 wird in den Auslieferungszustand zurückversetzt. Alle Konfigurationsdateien werden gelöscht, die BOOTmonitor-Einstellungen werden auf die Standardwerte gesetzt.
- (5) Default BOOTmonitor Parameters:
Sie können die Standardeinstellungen von **X1000s** BOOTmonitor verändern, z. B. die Baudrate für serielle Verbindungen.



Wenn Sie die Baudrate verändern (voreingestellt ist 9600 Baud), achten Sie darauf, daß das verwendete Terminal-Programm diese Baudrate verwendet. Wenn dies nicht der Fall ist, können Sie keine serielle Verbindung zu **X1000** herstellen!

12 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

12.1 SNMP-Shell-Kommandos

Auf **X1000** sind einige Programme vorinstalliert, die direkt von der SNMP-Shell aus gestartet werden können. Eine kurze Beschreibung der gebräuchlichsten Programme und die dazugehörige Kommandozeile, die Sie zum Starten der jeweiligen Programme in der SNMP-Shell eingeben, folgen:



Durch Eingabe von `?` wird eine Übersicht der wichtigsten Kommandos, die auf **X1000** verfügbar sind, 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 nächste 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.
- `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 414)
- `-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` = **X1000**'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 **X1000** zu öffnen.

- `-c <stknumber>`: Definiert den ISDN-Stack (falls mehrere ISDN-Karten genutzt werden).
- `-C`: Versucht, Komprimierung 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 **X1000s** Subsystemen anzuzeigen.

- `show`: Alle möglichen Subsysteme anzeigen, die auf Fehler untersucht werden können.
- `-q`: Keinen Zeitstempel vor jede Debugging-Meldung stellen.
- `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`: **X1000s** 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 12ten 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]`

X1000 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 **X1000** über Telnet, ISDN-Login oder seriell automatisch getrennt, wenn 15 Minuten lang keine Eingabe über die Tastatur erfolgt).

- `seconds`: Nach `seconds` Sekunden erfolgt der Autologout. Mit Eingabe von `t 0` deaktivieren Sie Autologout.

nslookup

`nslookup [-an] [-t <type>] [-w <sec>] [-r <ret>] ipaddr | name [<server>]`

Wird benutzt, um zu prüfen, wie ein Name oder eine IP-Adresse durch **X1000** oder einen anderen Name Server aufgelöst wird.

- `-a`: Zeigt alle erhaltenen Daten an.

- `-n`: Verhindert die Auflösung der angegebenen Name-Server-Adresse (ohne diese Option wird versucht, die Adresse des Name Servers aufzulösen).
- `-t <type>`: Anfragen der Art `<type>` ausführen. Mögliche Werte für `type`: 0, A, NS, MD, MF, CNAME, SOA, MB, MG, MR, NULL, WKS, PTR, HINFO, MINFO, MX, TXT, ANY oder eine beliebige Dezimalzahl.
- `-w <sec>`: `<sec>` Sekunden warten, bevor eine Anfrage erneut gesendet wird (Standardwert: 3).
- `-r <ret>`: Höchstens `<ret>` mal eine Anfrage senden (Standardwert: 5).
- `ipaddr`: Aufzulösende IP-Adresse.
- `name`: Aufzulösender Name.
- `<server>`: IP-Adresse des Name Servers, der befragt werden soll (Standardwert: 127.0.0.1). Es wird versucht, diese Name-Server-Adresse vom lokalen DNS Proxy auflösen zu lassen.



Durch Eingabe von `-?` (z.B. `netstat -?`) erhalten Sie meistens Hilfen zur Syntax.

Das Kommando `update` finden Sie in [Kapitel 9.3, Seite 381](#).

Weitere SNMP-Kommandos finden Sie in der Software Reference.

12.2 BRICKtools for Unix Kommandos

Die Programme bricktrace und capitrace sind in BRICKtools for UNIX auf der BinTec Companion CD enthalten. Sie werden durch Eingabe der folgenden Kommandos auf einem Unix-Rechner gestartet.

bricktrace

```
bricktrace [-h23aeFpiNtxs] [-T <tei>] [-c <cref>]
[-r <cnt>] [-H <host>] [-P <port>] <channel> <unit> <slot>
```

Wird benutzt, um ISDN-Meldungen (D- und B-Kanäle) zu verfolgen und auszuwerten.

- -h: hexadezimale Ausgabe.
- -2: Schicht-2-Ausgabe.
- -3: Schicht-3-Ausgabe.
- -a: Asynchronous HDLC (nur B-Kanal).
- -e: ETS300075 (Eurofile-Transfer)-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: **X1000** 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.
- 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 **X1000** gesendeten oder empfangenen CAPI-Meldungen werden angezeigt. Als Umgebungsvariable CAPI_HOST muß die IP-Adresse von **X1000** 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-Identifizier (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 Stecker-typ >>> **RJ45**.
- 10Base-2** Thin Ethernet-Anschluß. Netzwerkanschluß für 10 MBit-Netze mit dem Stecker-typ BNC. Zum Anschluß von Geräten mit BNC-Buchsen werden T-Verbindungsstücke eingesetzt.
- 1TR6** Im deutschen ISDN verwendetes D-Kanal-Protokoll. Heute gängigeres Protokoll ist das >>> **DSS1**.
- a/b** Standardschnittstelle für analoge Endgeräte (Telefon, Telefax Gruppe 2/3, analoge Modems). Nur bei BinTec-Routern mit integrierter >>> **PABX**.
- 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
- 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 **X1000** 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.

- Configuration Manager** Windows-Applikation (ähnlich dem Windows-Explorer), die SNMP-Kommandos benutzt, um die Einstellungen von **X1000** abzufragen und vorzunehmen. Die Applikation wurde vor der BRICKware Version 5.1.3 als DIME Browser bezeichnet.
- 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. **X1000** 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.
- DIME Browser** Alte Bezeichnung für ►► **Configuration Manager**.
- 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.
- 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.

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 **X1000** 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 **X1000**. Über ISDN-Login ist **X1000** 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 **X1000**. Kanalbündelung ist eine Methode, den Datendurchsatz zu erhöhen. Indem dynamisch (= bei Bedarf) oder statisch (= immer) ein zweiter **➤➤ B-Kanal** zur Datenübertragung hinzugeschaltet wird, verdoppelt sich der Durchsatz.

LAN Local Area Network (Lokales Netzwerk)

Räumlich eng begrenztes Netzwerk, das sich unter Kontrolle eines Besitzers befindet. Meist innerhalb eines Gebäudes/Firmensitzes.

MAC-Adresse Jedes Gerät im Netz ist über eine feste Hardware-Adresse (MAC-Adresse) definiert. Die Netzwerkkarte eines Geräts bestimmt diese weltweit eindeutige Adresse.

MIB Management Information Base

MIB ist eine Datenbank, die alle im Netz angeschlossenen managbaren Geräte und Funktionen beschreibt. Jede MIB (so auch die BinTec MIB) enthält herstellerspezifische Objekte. **➤➤ SNMP** setzt auf MIB auf.

Modem Modulator/Demodulator

Ein elektronisches Gerät. Wird verwendet, um digitale Signale in (analoge) Tonfrequenzsignale umzuwandeln und umgekehrt, so daß die Daten auf einer analogen Leitung übertragen werden können.

MPPC Microsoft Point-to-Point Compression

Verfahren zur **➤➤ Datenkompression**.

MPPE 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 **X1000**. 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 **X1000**) 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 **X1000** 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 **X1000** 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 **X1000** sind **➤➤ Multiprotokoll-Router** und dadurch in der Lage, mehrer Protokolle zu routen (z B. IP und IPX).

S₀-Anschluß Siehe **➤➤ ISDN-Basisanschluß**.

- S₀-Bus** Sämtliche ISDN-Anschlußdosen und der **NTBA** beim ISDN-Mehrgeräteanschluß. 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 **X1000**. 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).

- T-DSL** Produktname der Deutschen Telekom AG für ihre **DSL**-Dienstleistungen und Produkte.
- TE** Terminal Equipment
Endgerät am Teilnehmeranschluß, z. B. Telefon, Faxgerät oder Computer.
- 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	359
	Access Lists	338
	Activity Monitor	325
	Advanced Configuration	213
	Allgemeine PPP-Einstellungen	220
	Always On/Dynamic ISDN	233
	Anmelden	118, 328
	Anrufbeantworter einrichten	77
	Anschlüsse	402
	AO/DI	233
	Arbeitsspeicher	370
	ARP	261
	Aufstellen und Anschließen	37
	Auslieferungszustand	379
	Außendienstmitarbeiter	53
	Authentisierung	220, 330, 357
	Auto-Logout	365
B	Backroute Verification	356
	Bandwidth on Demand	226
	BinTec Companion CD	20
	Blowfish	359
	BOD	226
	BOOTmonitor	406
	BOOTP Relay Agent	295
	BOOT-Sequenz	406
	BRICKware installieren	47
C	Callback	330
	CAPI	94
	CAPI User Concept	216
	Channel Bundling	90, 224, 226
	Basiskonfiguration	224
	Erweiterte Konfiguration	226
	CHAP	220, 330

	CLID	329
	Closed User Group	332
	Compuserve	195, 198
	Credits Based Accounting System	317
D	Default-Route	187
	Delay after Connection Failure	223
	Denial-of-Service-Attacke	365
	DES	359
	DHCP-Server	98
	Dienst	94, 294, 338
	DNS	101, 253, 273
	Dokumentation	22
	Domain Name	273
	Dynamic IP Address Server	214
E	Eingehende Rufnummer überprüfen	329
	Einloggen	118, 328
	E-Mails	84
	Encryption	359
	Enkapsulierung	143
	Extended IP-Routing	357
F	Factory Reset	379
	Fax einrichten	77
	Fax empfangen	86
	Fax verschicken	84
	Festverbindung	146, 305
	Filter	107, 162, 338, 352
	Firmennetzanbindung	
	Allgemeines Beispiel	202
	Configuration Wizard	64
	Dial-in ohne Router	205
	Setup Tool	201
	Firmenniederlassung	52
	Flash-Speicher	370

G	Garantiebedingungen	24
	Grundlagen	89
H	HTTP-Statusseite	321
I	Incoming Call Answering	146
	Internetzugang	
	Compuserve	195
	Configuration Wizard	62
	Setup Tool	195
	T-Online	195
	Internet-Zugang testen	84
	IP-Adresse	98, 143
	Pool	214
	IPSec	305, 363
	IPX	298
	LAN-Schnittstelle	300
	WAN-Partner	301
	ISDN	90, 146
K	Kanalbündelung	90, 224, 226
	Keepalive Monitoring	263
	Kommandos	
	BRICKtools for Unix	417
	SNMP-Shell	410
	Kommunikationsanwendungen	51
	Komprimierung	93
	MS-STAC	259
	STAC	93, 259
	Van Jacobson Header Komprimierung	93, 259

Konfiguration	
E-Mails verschicken und empfangen	84
Faxe verschicken und empfangen	77
Partnernetz	73
PC einrichten	71
Remote	116
Remote-CAPI	69
RVS-COM Lite	77
Setup Tool	135
Sichern	211
Testen	84
Unter Windows	55
Vorbereiten	40
Weiterführende	213
Konfigurationsdateien verwalten	370
Konfigurationsmöglichkeiten	
Übersicht	121
L LAN-LAN-Kopplung	
Configuration Wizard	64
Setup Tool	201
LAN-Schnittstelle	143
Layer 1 Protocol	247
LEDs	399
Lieferumfang	19
Lizenz eintragen	138
Lizenzkarte	40
Lokale Filter	352
Lösungsszenarien	49
M Memory	370
MIB	109
Monitorfunktionen im Setup Tool	313
MPPE	359
MS-STAC	259
N Namensauflösung	101, 253, 273

	NAT	193, 333
	NetBIOS	101, 107, 253
	Network Address Translation	193, 333
	Netzmaske	143
	Novell-Netzwerke	298
P	PAP	220, 330
	Partnernetz	73
	Paßwortänderung	128
	Paßwörter eintragen	140
	PC einrichten	71
	Pick-Up-Service	24
	Pin-Zuordnung	403
	Port	294, 338
	PPP-Einstellungen	220
	PPTP	305, 363
	Produktmerkmale	396
	Proxy ARP	261
R	RAM	370
	Regel	338
	Remote-CAPI	69, 94, 332
	RIP	256
	Routen	104
	Router-Grundkonfiguration	
	Configuration Wizard	58
	Setup Tool	137
	Routing Information Protocol	256
	Routing-Eintrag	187
	Rufnummern	90
	RVS-COM Lite	77
S	SAFERNET	307

Setup Tool	
Bedienung	122
Grundkonfiguration	135
Menüstruktur	130
Monitorfunktionen	313
Shorthold	90, 182
Sicherheitsmechanismen	307
Abhörsicherung	359
Besonderheiten	365
Checkliste	367
Überwachen von Aktivitäten	308
Zugangssicherung	328
SNMP	109
Software-Update	381
STAC	259
Startup-Verhalten	365
Syslog-Messages	308
Systemdaten eintragen	140
Systemvoraussetzungen	23
Systemzeit	269
T	
TAF	357
Taschengeldkonto	317
TCP/IP-Protokoll installieren	45
TCP/IP-Protokoll prüfen	44
Technische Daten	395
Time-Server	269
Token Authentication Firewall	357
T-Online	195
Transit Network	249
Trouble Shooting	385
Hilfsmittel	386
IPX-Routing	392
ISDN-Verbindungen	389
System-Fehler	388
U	
Update	381

V	Van Jacobson Header Komprimierung	259
	Verschlüsselung	359, 363
	Virtual Private Network (VPN)	305, 363
	VPN	305, 363
W	WAN-Partner einrichten	169
	WAN-Schnittstelle	146
	Windows-Netzwerk einrichten	43
	WINS	101, 253, 273
X	X.31 TEI	222
Z	Zugangsmöglichkeiten	112
	ISDN	116
	LAN	115
	Serielle Schnittstelle	113
	Zugangssicherung	328
	Zusatzlizenz	305

