

HERMES-PRO/X

Handbuch

HERMES-PRO/X

Handbuch

Version 1.1

MULTIDATA

Erklärung zum Copyright

AIX[®] ist ein eingetragenes Warenzeichen der International Business Machines Corporation; UnixWare[®] ist ein eingetragenes Warenzeichen der Novell Inc. Windows 95, Windows 98 und Windows NT[®] sind eingetragene Warenzeichen der Microsoft Corporation.

Erklärung zu den Eigentumsrechten

Die mit HERMES-PRO/X mitgelieferte Software und das dazugehörige Handbuch unterliegt dem Urheberrecht ©Copyright 1999 der MULTIDATA GmbH. Alle Rechte vorbehalten. Der Käufer erhält das nicht ausschließliche Recht, diese Software auf einem Computer zu nutzen. Dieses Recht ist nicht übertragbar, vermietbar oder verleihbar.

Es ist untersagt die Software und das zugehörige Handbuch ohne vorherige ausdrückliche schriftliche Zustimmung der MULTIDATA GmbH in irgendeiner Form oder durch irgendwelche Medien weder ganz noch auszugsweise zu kopieren, zu verändern, zu vermieten, zu veröffentlichen, umzugestalten oder von einem Hauptspeicher auf einen anderen Datenträger zu übertragen oder zu nutzen.

Diese Software darf aber zur eigenen Datensicherung kopiert und archiviert werden. Fehlerhafte Disketten werden im Rahmen der gesetzlichen Garantiebestimmungen von der MULTIDATA GmbH ersetzt.

Änderungen an der hier beschriebenen Software und dem Handbuch bleiben jederzeit und ohne vorherige Ankündigung vorbehalten.

Haftungsbegrenzung

Die Software und Dokumentation wurden mit aller gebotenen Sorgfalt entwickelt und geprüft.

Die MULTIDATA GmbH übernimmt keinerlei Haftung für Folgeschäden jeder Art, die sich aus der Benutzung des Routers HERMES-PRO/X, der mitgelieferten Software und der dazugehörigen Dokumentation ergeben, sofern sie nicht aufgrund von Vorsatz oder grober Fahrlässigkeit seitens der MULTIDATA GmbH entstanden sind.

Inhaltsverzeichnis

1	Kurzbeschreibung	7
1.1	Leistungsmerkmale.....	8
1.2	Lieferumfang.....	9
2	Einführung in TCP/IP.....	11
2.1	Geschichte.....	11
2.2	Begriffsbestimmung.....	13
2.2.1	Internet Protocol (IP).....	13
2.2.2	Transmission Control Protocol (TCP).....	16
2.2.3	Internet Control Message Protocol (ICMP).....	17
2.3	Subnetze.....	18
2.4	Routing.....	20
2.5	Point-to-Point Protocol (PPP).....	22
2.6	Network Address Translation (NAT).....	23
2.6.1	LAN zu WAN.....	23
2.6.2	WAN zu LAN.....	24
2.6.3	Verbindungsüberwachung.....	25
3	Installation.....	27
3.1	Benötigte Informationen.....	27
3.2	Vorraussetzungen zum Anschluß von HERMES-PRO/X.....	28
3.3	Aufstellen und Anschließen.....	29
3.4	Bedeutung der LED Anzeigen.....	30
3.5	Erste Schritte.....	30
4	Ethernet-Switch.....	33
4.1	Beschreibung der Funktionseinheit.....	33
5	USB Schnittstelle.....	35
5.1	Start mit spezieller Konfiguration.....	35
5.2	Verwendung zur Laufzeit.....	36
6	Routerfunktion.....	37
6.1	Struktur.....	37
6.2	Die IP-Schnittstelle.....	37
6.3	Der Routing-Prozeß.....	37
6.4	Datenübertragung.....	38
6.5	Verbindungsabbau.....	38
6.6	Routing.....	39
6.7	Besondere Adressen.....	40

Inhaltsverzeichnis

6.8	ISDN Schicht 2 und Schicht 3 Protokolle	40
6.9	Schutz vor Mißbrauch.....	40
6.10	PPP über ISDN.....	41
6.11	Callback.....	41
6.12	Kanalbündelung.....	43
6.13	Debugging	44
6.14	Interoperabilität.....	44
7	Firewall-Mechanismus	45
7.1	Konfigurationsmöglichkeiten.....	46
7.2	Arbeitsweise von IP-Tables	47
7.3	Chains für HERMES-PRO.....	49
7.4	Die Stationen eines Pakets	51
7.5	Konfigurationsmenüs.....	52
7.5.1	IP Tables (Firewall).....	52
7.5.2	New IP Tables Set.....	52
7.5.3	Edit IP Tables Set.....	53
7.6	Format der Konfigurationsdatei	56
7.6.1	Abschnitt [IPTABLESSECTIONS]	56
7.6.2	Abschnitt [<i>Tabellenname_nnn</i>]	56
7.7	Portdefinition.....	59
7.8	Protokolldefinition	59
7.9	Tipps zur Konfiguration.....	60
7.10	Konfigurationsbeispiele	61
8	IPSec und VPN.....	63
8.1	Anwendungsfälle	64
8.2	DynDNS.....	65
8.3	Interoperabilität.....	66
8.3.1	Dynamische IP-Adressen	66
8.3.2	Parameteraushandlung mit ISAKMP.....	67
8.3.3	Manuelle Schlüsselkonfiguration	69
8.3.4	Dead Peer Detection (DPD)	69
8.3.5	NAT-Traversal	69
8.4	Format der Konfigurationsdatei	71
8.4.1	Abschnitt [IPSecn]	71
8.4.2	Abschnitt [VPNRoutern].....	74
8.4.3	Abschnitt [DynDNS].....	75
8.5	Firewalleinstellungen	77
9	CAPI-Serverfunktion	78
9.1	Grundlagen.....	78
9.2	Client.....	78
9.2.1	Konfiguration von capi2032.dll.....	79

9.2.2	16-Bit Anwendungen.....	79
9.3	Server.....	80
10	Konfiguration	81
10.1	Konfiguration über einen Web-Browser.....	81
10.1.1	General Router.....	82
10.1.2	Accounting Restricted Dialout.....	84
10.1.3	Hosts Database	85
10.1.4	IP Interfaces.....	86
10.1.5	DHCP Server	87
10.1.6	ISDN Peer Stations.....	89
10.1.7	PPP Sections	91
10.1.8	LCP Sections	92
10.1.9	IPCP Sections.....	93
10.1.10	CHAP Sections	94
10.1.11	IP-Tables (Firewall).....	95
10.1.12	Port Forwarding.....	95
10.1.13	IPSec and VPN	96
10.1.14	DynDNS	97
10.1.15	Show active ISDN/DSL Connections	97
10.1.16	Show active TCP/UDP/ICMP Connections.....	98
10.1.17	Show Logfile.....	99
10.1.18	Update Router Image.....	99
10.1.19	Trace Parameters	99
10.2	Konfigurationsdateien	101
10.2.1	Abschnitt [ISDND]	101
10.2.2	Abschnitt [peer].....	104
10.2.3	Abschnitt [peerPPP].....	107
10.2.4	Abschnitt [PeerLCP].....	108
10.2.5	Abschnitt [peerIPCP].....	109
10.2.6	Abschnitt [peerCHAP]	110
10.2.7	Abschnitt [INTERFACES]	111
10.2.8	Abschnitt [DHCPRange].....	111
10.2.9	Abschnitt [DHCPMapping <i>n</i>]	112
10.2.10	Abschnitt [PortForwarding <i>n</i>].....	113
10.2.11	Abschnitt [TRACE]	114
11	Betriebssystem des Routers	115
11.1	Leistungsumfang.....	115
11.2	HERMES-spezifische Hilfsprogramme	117
11.2.1	flash_tool.....	117
11.2.2	testhsc.....	118
11.2.3	gpf2	120

Inhaltsverzeichnis

11.2.4	fppp.....	121
11.2.5	fascii	122
11.2.6	getcfg.....	122
A	Konfigurationsbeispiele.....	123
A.1	Callback.....	123
A.1.1	HERMES H1 ruft HERMES H2 mit CLIP.....	123
A.1.2	HERMES H1 ruft HERMES H2 mit PPP/LCP	123
A.1.3	WinNT ruft HERMES H2 mit CBCP	124
A.2	Accounting Restricted Dialout	125
B	Tabellen	127
B.1	Tabelle der wichtigsten CIP Werte	127
B.2	Tabelle der B-Protokolle	128
B.2.1	Schicht 1 Protokolle.....	128
B.2.2	Schicht 2 Protokolle.....	128
B.2.3	Schicht 3 Protokolle.....	129
B.3	CAPI Fehlermeldungen	130
B.4	ISDN Debug-Informationen	134
B.5	Steuerung der Log-Ausgaben	135
C	Troubleshooting	137
C.1	Zugang zur Web-Konfiguration	137
C.2	Notbetrieb	137
C.3	Verbindungsaufbau	138
D	Begriffe und Abkürzungen	141
E	Literaturverzeichnis	145
F	Garantiebedingungen	147

1 Kurzbeschreibung

HERMES-PRO/X realisiert einen kosteneffektiven standalone LAN/WAN-Router. Er basiert auf der bewährten Routing-Software HERMES-IP und den ISDN Protokollstacks von MULTIDATA.

Die Vorteile dieses standalone Routers sind die Unabhängigkeit vom Betriebssystem und der Rechnerplattform und die benutzerfreundliche Installation und Konfiguration.

HERMES-PRO/X integriert einen Switch mit fünf LAN-Ports, die 10 Mbit/s und 100 Mbit/s Ethernet unterstützen.

Standardmäßig stellt HERMES-PRO/X einen Remote CAPI Server zur Verfügung. Im Lieferumfang von HERMES-PRO/X ist eine Remote CAPI (*capi2032.dll*) für Windows 95/98/NT/2000/XP Clients enthalten. Für den Einsatz unter UNIX wird eine Klassenbibliothek (*capi2lib.o*) bereitgestellt, welche die Funktionalität eines Remote CAPI Clients realisiert. Somit können CAPI Dienste von Kommunikationsanwendungen im Netz genutzt werden.

HERMES-PRO/X unterstützt TCP/IP-Routing und PPP mit den Authentisierungsverfahren CHAP und PAP. Eine "Stateful Inspection Firewall" ist integriert. Ein weiteres Sicherheitsmerkmal sind die integrierten Rückrufmechanismen. Ein Accounting-Mechanismus erlaubt die Überwachung aktiver Verbindungen. Umfangreiche Methoden zur Gebührenkontrolle können genutzt werden.

1.1 Leistungsmerkmale

Software:

- statisches und dynamisches IP-Routing über ISDN und PPPoE
- Unterstützung beider B-Kanäle der S₀-Schnittstelle
- intelligentes Leitungsmanagement (Short-Hold-Modus)
- PPP mit Authentisierungsverfahren CHAP und PAP
- Rückruf, gesteuert über D-Kanal oder PPP
- Firewall-Funktionalität
- Network Address Translation
- DHCP Server
- Port Forwarding
- VPN Unterstützung
- Management über Web-Browser oder telnet
- Update der Firmware über Web-Browser
- Remote CAPI 2.0 für Windows 9x/NT/2000/XP und UNIX/Linux
- Kommunikation mit V.23 Modems und Fax Gruppe 3 Geräten
- Vermittlungsprotokoll E-DSS1
- Gebührenkontrolle über ARD

Hardware:

- Integrierter Switch mit fünf 10Base-T/100Base-TX Ports, autom. Crossover, QoS und VLAN-Funktionalität
- Zweite Ethernet-Schnittstelle als WAN-Port
- ISDN Anschluß über S₀-Schnittstelle
- USB Host Anschluss
- 32 Bit PowerPC mit 400 MHz
- 64 MB SDRAM, 16 MB Flash-ROM
- vielfältige Statusanzeigen über LEDs
- Steckernetzteil (85VAC-264VAC)
- geringer Leistungsverbrauch (max. 7 Watt), ohne Lüfter
- kompakte Bauform (B*H*T): 222 mm*38 mm*160 mm

1.2 Lieferumfang

Zum Lieferumfang gehören:

- der Router HERMES-PRO/X mit Steckernetzteil und dieses Handbuch
- ein 3 m langes gelbes ISDN S₀-Kabel, ein rotes Ethernetkabel.

MULTIDATA behält sich jedoch das Recht vor, Änderungen am Lieferumfang ohne Vorankündigung vorzunehmen.

2 Einführung in TCP/IP

TCP/IP-Implementierungen sind heute vom Großrechner bis zum PC, unabhängig vom Hersteller, von der Hardware und vom Betriebssystem verfügbar. Dies hat TCP/IP die Aufmerksamkeit eines großen Publikums beschert, das weit über das ursprüngliche Interesse in der U.S.A. hinaus geht. Weltweit lösen damit heute Anwender die Probleme, die bei der Datenübermittlung zwischen Rechnern verschiedener Hersteller entstehen.

TCP/IP ist eine Abkürzung für viele verschiedene Standards mit vielen verschiedenen Merkmalen und Funktionen. Dieses Kapitel gibt einen Rückblick auf die Entstehung von TCP/IP und stellt die wichtigsten Komponenten vor.

2.1 Geschichte

Im Jahre 1969 startete die Advanced Research Projects Agency (ARPA), eine Abteilung des Department of Defense (DoD), ein Entwicklungsprojekt mit dem Namen ARPANET. Dieses Netz sollte der in der damaligen Zeit aufkommenden Forderung der Universitäten und Forschungseinrichtungen nach einer landesweiten Nutzung der vorhandenen Rechnerkapazitäten gerecht werden. Es sollten Techniken für eine zuverlässige herstellerunabhängige Datenkommunikation entwickelt werden. Ziel war es also, einen allgemeinen Standard zu entwickeln, der es erlaubte, unterschiedliche Rechner und auch Netze zu verbinden. Damit konnte ein Informationsaustausch zwischen allen Organisationen erfolgen, die über ein eigenes Computernetz verfügten. An dieser Neuentwicklung arbeiteten Universitäten, Forschungseinrichtungen und militärische Einrichtungen.

Die Anfänge bestanden aus mehreren Knotenrechnern, die über gemietete Leitungen zu einem Netz verbunden wurden. Durch diese Knotenrechner, sogenannte Internet Message Processors (IMP), war der Zugang zum ARPANET für einen einzelnen Hostrechner möglich. Als IMPs wurden ursprünglich Honeywell DDP-516 Minicomputer mit 12 K 16 Bit Wortspeicher

eingesetzt. Später ersetzte man diese Computer durch größere Maschinen, die dann PSNs (Packet Switch Nodes) genannt wurden. Ursprünglich konnten die IMPs nur einen bis maximal vier Hostrechner bedienen. Diese Grenze ist im Laufe der Jahre jedoch um einige Größenordnungen heraufgesetzt worden.

Im Jahre 1972 wird die ARPA in DARPA (Defense Advanced Research Agency) umbenannt, da diese Abteilung vor allen Dingen für militärische Projekte zuständig war. Das ARPANET selbst war inzwischen so erfolgreich, daß aus dem ehemals experimentellen Netz 1975 ein Benutzernetz entstand. Die Verwaltung des Netzes wurde dem DCA (Defense Communications Agency) übertragen. Trotzdem wurde die Forschung und Entwicklung am ARPANET weiterbetrieben.

Bereits in den Anfangsjahren (Beginn der 70er Jahre) erkannte man, daß die damals verwendeten Protokolle den Anforderungen nicht mehr gerecht wurden, so daß die Entwicklung einer neuen Protokollbasis gestartet wurde. Folgende Kriterien sollte die Protokollarchitektur beinhalten:

- Unabhängigkeit der unterschiedlichen Funktionsweisen bzw. Architekturen verschiedener Netze oder Computersysteme untereinander
- globale Verbindungsmöglichkeiten im gesamten Netz
- Endpunkt orientierte Verbindungen mit Quittungen
- standardisierte Anwendungsprotokolle

Anfang der 80er Jahre wurde für das ARPANET und andere DoD-Netze eine neue Protokollfamilie eingeführt, der DARPA-Internet-Protokollsatz, auch TCP/IP-Protokollsatz oder einfach kurz TCP/IP (Transmission Control Protocol/Internet Protocol) genannt. Anschließend wurde 1982 die Firma Bolt, Beranek und Newman (BBN) beauftragt, TCP/IP im UNIX-System der Universität von Kalifornien in Berkeley zu implementieren. Diese Implementierung in das bekannte UNIX 4.2BSD System (Berkeley System Distribution) hatte zur Folge, daß der entsprechende Quellcode damit ab 1983 als Public Domain Software frei zugänglich wurde. Dies führte zu einer sehr schnellen und weiten Verbreitung der Protokolle.

1984 wurde das alte ARPANET in zwei getrennte Netze gespalten. Zum einen in MILNET, das nur für militärische Zwecke genutzt werden sollte und ARPANET für Forschungszwecke. In dieser Zeit wurde auch immer häufiger der Begriff Internet gebraucht. Der Begriff Internet bezog sich auf das gesamte Netz, sowohl MILNET als auch ARPANET. Mittlerweile ist das Internet immer mehr in den Brennpunkt kommerzieller und auch privater

Interessen gerückt und ist wenigstens in den informationstechnisch-orientierten Bereichen ein wertvolles Hilfsmittel und nicht mehr wegzudenken.

2.2 Begriffsbestimmung

Der Begriff TCP/IP bezeichnet zwei verschiedene Ebenen der Protokollhierarchie. Die Schicht IP (Internet Protocol) ist für den Transport und die Vermittlung von Datenpaketen zuständig. Dies wird auch als Netzebene bezeichnet. Die darüberliegende Schicht TCP (Transmission Control Protocol) ist nur eine von vielen möglichen darüberliegenden Protokollen, die IP als Netzschicht verwenden. Es hat sich eingebürgert, von TCP/IP zu sprechen, aber eigentlich IP zuzüglich weiterer Protokollschichten zu meinen. Diese sind unter anderem:

- UDP (User Datagram Protocol)
- ICMP (Internet Control Message Protocol)
- TCP .

Das oft zitierte OSI-Referenzmodell ist auf TCP, UDP etc. und auch auf IP nicht bzw. nur teilweise anwendbar, weil es sich um nicht mit OSI (Open Systems Interconnection) konforme Protokollschichten handelt. Im übrigen wurden diese Protokolle ca. 10 Jahre vor dem OSI-Referenzmodell entworfen.

2.2.1 Internet Protocol (IP)

Eine IP-Adresse der IP Version 4 (Ipv4) ist ein 32-Bit Wert, der innerhalb des Netzes eindeutig sein muß. Er identifiziert die Verbindung eines Endsystems oder Routers im Netz. Existiert mehr als eine Netzverbindung zu normalerweise unterschiedlichen Netzen, so muß jede dieser Verbindungen eine eigene IP-Adresse haben. Im Gegensatz zu anderen Adressierungsschemata (z.B. Telefonnummern), sind IP-Adressen nicht hierarchisch und geben nicht notwendigerweise Auskunft über den geographischen Standort. Eine IP-Adresse setzt sich aus zwei Komponenten, einem Netzadriß- und einem Endsystemadrißanteil, zusammen. Konvention ist, daß die IP-Adresse in dezimaler Punktschreibweise notiert wird. Hierbei werden jeweils 8 aufeinanderfolgende Bits (Oktett) der Adresse in eine Dezimalzahl zwischen 0 und 255 umgewandelt, die jeweils durch einen Punkt voneinander getrennt werden. Anhand der höherwertigen Bits des ersten Oktetts

der IP-Adresse erfolgt eine Aufteilung in 5 Adreßklassen, wie in Abb. 2.1 dargestellt.

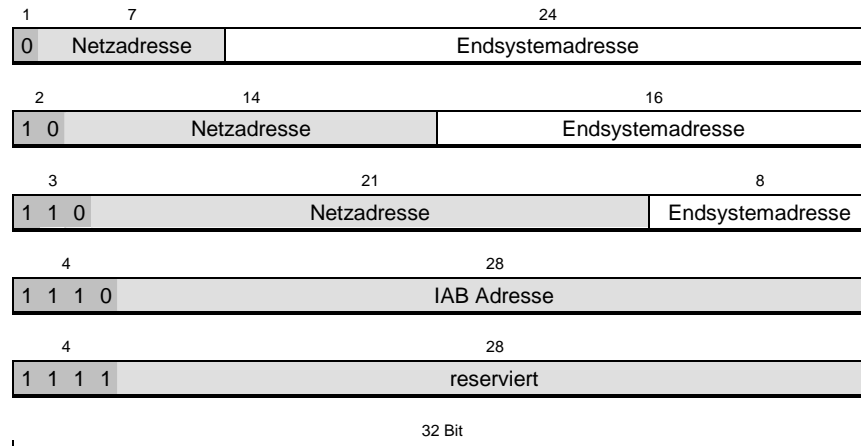


Abb. 2.1: Aufteilung in IP-Adreßklassen

Hierbei stellen die dunkelgrau unterlegten Felder die verwendeten Klassenbits innerhalb der Netzadresse dar, die Werte oberhalb des jeweiligen Adreßanteils geben die Anzahl der für Netz- und Rechneradresse zur Verfügung stehenden Bits an. Die ersten drei Klassen (A, B und C) stehen für die normale Adressierung und für die Kommunikation von Endsystem zu Endsystem zur Verfügung. Hier werden für den Netzanteil der Adresse 1, 2 bzw. 3 Byte verwendet. Adressen der vierten Klasse (D) sind für spezielle IAB-Protokolle (Internet Architecture Board) und Adressen der fünften Klasse (E) für zukünftige Verwendungszwecke reserviert und stehen nicht allgemein zur Verfügung.

Nehmen wir z.B. die IP-Adresse 194.34.7.5, dann ist der Netzanteil der Adresse 194.34.7. Für den lokalen Anteil dieser Adresse der Klasse C verbleibt somit ein Byte mit dem Wert 5, der das Endsystem (Host) identifiziert.

TCP/IP-Anwender müssen mit den hier vorgestellten Adreßklassen vertraut sein, um die jeweiligen Restriktionen auf die Größe des Netzes zu kennen. Tab. 1 faßt daher die Kapazitäten der fünf IP-Adreßklassen bezüglich der zur Verfügung stehenden Netzadressen, Endsystemadressen pro Netz und

deren Netzadreibereich nochmals zusammen. Durch Strukturierung der Adressen sowie durch Spezialfunktionen kann die Anzahl der tatsächlich möglichen Endsystemadressen weiter eingeschränkt sein.

Klasse	Netze	Rechner	Erster Wert	Letzter Wert
A	126	16.777.214	1	126
B	16.382	65.534	128.1	191.254
C	2.097.150	254	192.0.1	223.255.254
D	-	268.435.454	224.0.0.0	239.255.255.254
E	-	268.435.454	240.0.0.0	255.255.255.254

Tab. 1: Kapazität der verschiedenen IP-Adreßklassen

Absender und Empfänger müssen natürlich nicht am selben lokalen Netz (physisch) angeschlossen sein, sondern es reicht, wenn mindestens ein Teilnehmer an dem lokalen Netz Zugang zu weiteren Netzteilen hat. Dieser Knoten übernimmt dann die Weitervermittlung von Datenpaketen. Der Transport solcher Pakete erfolgt anhand der Zieladresse. Dabei wird das Paket von Netzknoten zu Netzknoten weitergereicht (Store and Forward), bis es den Empfänger erreicht hat bzw. bis der Weitertransport wegen fehlender Wege nicht mehr möglich ist. Die Information, über welchen Weg ein Datenpaket zum Ziel gelangen kann, wird aus dem Netzteil der Adresse abgeleitet. Der Absender kann nicht direkt feststellen, ob ein Transportweg zu der Zieladresse existiert oder nicht, denn die Weiterleitung der Datenpakete, eine gegebenenfalls notwendige Fragmentierung in kleinere Pakete bzw. das Zusammensetzen fragmentierter Pakete und auch eine (möglicherweise) dynamisch erfolgte Änderung der Pfade zum Ziel sind Sache des jeweiligen Knotens.

Version	IHL	Diensttyp	Gesamtlänge	
Kennung			Flags	Fragment-Offset
Lebensdauer		Protokoll	Kopf-Prüfsumme	
Absender-IP-Adresse				
Empfänger-IP-Adresse				
Optionen				Füllzeichen

32 Bit

Abb. 2.2: IP-Header

2.2.2 Transmission Control Protocol (TCP)

Der Hintergedanke bei TCP ist, eine virtuelle Verbindungsmöglichkeit zwischen zwei Rechnern, genauer zwischen zwei Anwendungen auf den Rechnern zu etablieren. Diese Verbindung sollte:

- einen sicheren Datentransport gewährleisten
- die Beibehaltung der Paketreihenfolge sicherstellen
- die Anwendungen eindeutig identifizieren.

Das ursprünglich im ARPANET entwickelte Protokoll NCP erfüllte vor allem die gestiegenen Anforderungen an die Sicherheit der Übertragung nicht, da mit dem Anwachsen der Netzknotenzahlen und vieler unterschiedlicher Transportwege und -medien die Übertragungsfehlerrate zunahm. Deshalb wurde TCP entwickelt. TCP ist für die Sicherung der Zustellung von Paketen zuständig, quittiert den Empfang (IP quittiert nicht) von Paketen und sorgt gegebenenfalls für eine Wiederholung von verlorengegangenen Daten. Bei der Verwendung von TCP wird jeder Anwendung eine 16 Bit lange Adresse, die sogenannte Portnummer zugewiesen. Dieses kann fest oder variabel geschehen. Beispielsweise haben unter anderem folgende Anwendungen (auch Dienste genannt) fest zugewiesene Nummern:

Anwendung	Beschreibung	Port
ftp	Dateitransfer	20, 21
smtp	E-Mail	25
telnet	Terminalanwendung	23
http/www	World Wide Web	80
dns	Domain Name Service	53
pop3	E-Mail	110

Tab. 2: Beispiel fest zugeordneter Portnummern

Wenn also beispielsweise auf dem System mit der IP-Adresse 194.34.7.5 ein File-Transfer gewünscht wird, so wird eine TCP/IP-Verbindung mit dem Port 21 aufgenommen, d.h. in einem IP Paket wird als Datenteil ein TCP-Paket mit der Zielportnummer 21 versendet. Der Absender (z.B. 100.100.100.100) wiederum hat sich dynamisch eine für den eigenen Rechner eindeutige Portnummer (1444) besorgt, so daß die Kombination aus

- Absender IP und Absender Portnummer, 100.100.100.100/1444

- Empfänger IP und Empfänger Portnummer, 194.34.5.7/21
eindeutig die Verbindung charakterisiert.

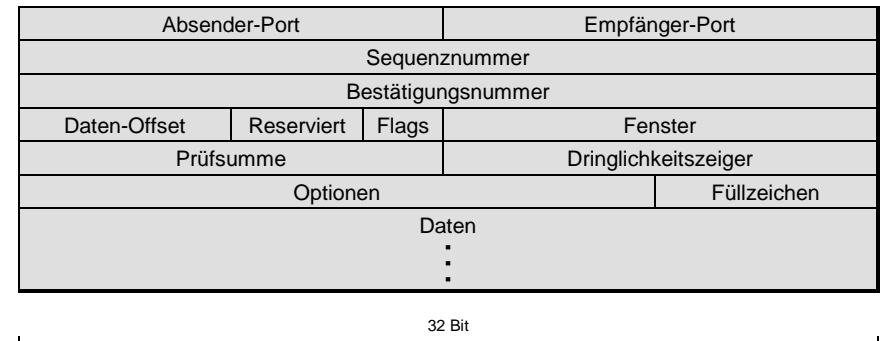


Abb. 2.3: TCP-Paket

Eine zweite File-Transferverbindung unterscheidet sich wenigstens bei der Portnummer des Absenders, also beispielsweise einer weiteren dynamisch zugewiesenen Portnummer 1456, so daß sich zwei neue, unterschiedliche Adreßpaare ergeben:

- Absender IP und Absender Portnummer, 100.100.100.100/1456
- Empfänger IP und Empfänger Portnummer, 194.34.5.7/21.

Damit ist die Zuordnung zu der entsprechenden Anwendung (oder einer zweiten Instanz derselben) jederzeit möglich und das Datenpaket kann der richtigen Anwendung übergeben werden. Dabei sorgt also jetzt TCP für die sichere Auslieferung der Daten, erzeugt Quittungen und Wiederholungen und stellt auch die Reihenfolge der Pakete sicher. Für den File-Transfer selbst ist das Anwendungsprogramm (FTP) zuständig, welches selbst wiederum ein Protokoll aufsetzt, um den Dateinamen und den Dateinhalt zu übertragen und weitere spezielle Funktionen zu realisieren.

2.2.3 Internet Control Message Protocol (ICMP)

Da ja die Weiterleitung von Paketen Sache des jeweiligen Netzknotens ist, gibt es ein weiteres Protokoll, welches Informationen zu der Weiterleitung von Paketen (Routinginformationen) übermitteln kann. ICMP-Pakete werden natürlich als IP-Pakete verpackt. Dabei können unter anderem die folgenden Informationen übermittelt werden:

- Ziel nicht erreichbar (es existiert kein Pfad zum Ziel)
- Zeitüberschreitung (eigentlich Zählerüberlauf, zu viele Knoten passiert)
- Echo Anforderung bzw. Antwort (Verbindungstest)
- Paketumleitung (Neuer Knoten für Zieladresse zuständig)

Dadurch ist also wenigstens eine rudimentäre Funktionalität für die Vermittlung, den Test bzw. auch für die Änderung von Routinginformationen gegeben. Jeder Netzknoten sollte wenigstens ICMP beherrschen. Darüber hinaus gibt es natürlich weitere Protokolle, die sehr viel komplexere Zusammenhänge bzgl. der Routinginformationen darstellen können.

2.3 Subnetze

Bei einer IP-Adresse stehen, je nach Klasse, ein, zwei oder drei Bytes für Endsystemadressen zur Verfügung. Selbst bei einem vergleichsweise kleinen Netz der Klasse C macht es aus den verschiedensten Gründen häufig schon Sinn, die bis zu 254 Endsysteme nicht innerhalb des selben Netzes zu betreiben. Unterstützt der Routing-Mechanismus Subnetzmasken werden ein oder mehrere Bits der Endsystemadresse dazu verwendet, den Adreßraum der Netzadresse zu erweitern und diesen auf mehrere physische, durch Router getrennte Subnetze zu verteilen. Hierbei wird aus der IP-Adresse anhand der gesetzten Bits der Netzmaske die Netzadresse ermittelt und den Ports eines Routers unterschiedliche Subnetznummern zugewiesen.

Die Konstruktion von Subnetzen wird jedoch durch folgende Konventionen limitiert:

- um Konflikte mit manchen Softwareprodukten zu vermeiden, ist es empfehlenswert, die Bits der Maske vom höchstwertigen zum niederwertigsten Bit lückenlos zu setzen
- eine Subnetznummer, die aus lauter Nullen besteht, darf nicht verwendet werden
- eine Subnetznummer, die aus lauter Einsen besteht, ist für das Rundsenden (Broadcast) an alle Subnetze des Netzes reserviert
- eine Endsystemadresse, die aus lauter Einsen besteht, ist für das Rundsenden an alle Endsysteme eines spezifischen Subnetzes oder an alle Subnetze der selben Netznummer reserviert. Die Notierung in dezimaler Schreibweise erschwert es, dies zu erkennen.

Dies schränkt den Bereich der verwendbaren Adressen ein; weiter als man zunächst vermutet.

Für Subnetze der Klasse C stehen dadurch lediglich zwei praktikable Unterteilungen zur Verfügung:

- 14 Netze mit 14 Endsystemen (Netzmaske 255.255.255.240)
- 6 Netze mit 30 Endsystemen (Netzmaske 255.255.255.224).

Letztere Möglichkeit wurde nochmals anhand von Tab. 3 und Tab. 4 dargestellt:

	Binär	Dezimal
IP-Adresse	11000010 00100010 00000101 10100101	194.034.005.165
Netzmaske	11111111 11111111 11111111 11100000	255.255.255.224
Netzadresse	11000010 00100010 00000101 10100000	194.034.005.160

Tab. 3: Beispiel für eine Subnetzmaske in einem Klasse C Netzwerk

Subnetz	Erstes Endsystem	Letztes Endsystem
x.y.z.32	x.y.z.33	x.y.z.62
x.y.z.64	x.y.z.65	x.y.z.94
x.y.z.96	x.y.z.97	x.y.z.126
x.y.z.128	x.y.z.129	x.y.z.158
x.y.z.160	x.y.z.161	x.y.z.190
x.y.z.192	x.y.z.193	x.y.z.222

Tab. 4: Beispiel eines Adreßraums eines Subnetzes

Die Einrichtung von Subnetzen verbessert die Kontrolle über den zur Verfügung stehenden Adreßraum, indem sie die normale Kapazität der Endsystemadressen auf eine bestimmte Anzahl von Subnetzen aufteilt. Bei sorgfältiger Planung wird hierdurch der Ausbau und die Anpassung des Netzes vereinfacht. Auch wenn man sich entscheidet, keine Subnetzadressierung zu verwenden, wird sich die Hardware dennoch dieser Technik bedienen und entsprechend der Adressen der Klasse A, B oder C automatisch die korrekte Standardmaske festlegen.

Mit der Einführung von CIDR (Classless Interdomain Routing) wird das Konzept der Adreßklassen überflüssig. Wird dieses Konzept von der Software unterstützt, ist es möglich jede beliebige Maske mit jedem Adreßbereich zu verwenden und auch die erste und letzte mögliche Netznummer zu nutzen.

2.4 Routing

Wenn zwei Systeme miteinander kommunizieren wollen, die nicht mit dem selben Netzwerk verbunden sind, müssen diese herausfinden auf welchem Weg die Verbindung hergestellt werden kann. Jedes System hat dazu eine eigene Routing-Tabelle in der festgehalten ist, welche Verbindungen (Netz- und Subnetzadressen) zu anderen Netzen bestehen. Meistens ist es so, daß in der Routing-Tabelle lediglich der Sprung zum nächsten Zwischenziel (Router) auf dem Weg zum Empfänger eingetragen ist. Als Router kann hierbei jedes System, das an mehrere Netze angeschlossen ist, fungieren. Häufig wird jedoch eine speziell für diese Aufgabe optimierte Hardware und entsprechende Routing-Software verwendet. Da Router aktive Teile von TCP/IP-Netzen sind, müssen sie bei der Netzverwaltung als Teil des IP-Adressierungsschemas behandelt werden.

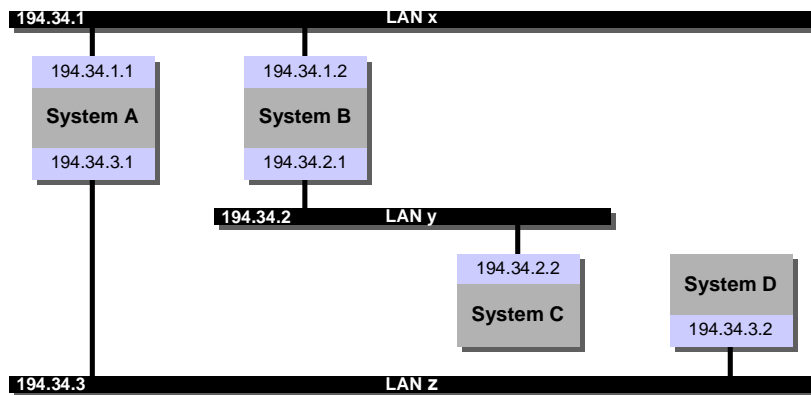


Abb. 2.4: Beispiel eines vernetzten Systems

Bei der Auswahl von Routen unterscheidet man zwischen statischen und dynamischen Verfahren. Im ersten Fall werden vom Netzverwalter eine begrenzte Anzahl von Routen und Alternativrouten festgelegt und in den Router geladen. Tab. 5 auf der folgenden Seite zeigt ein Beispiel einer

solchen Routing-Tabelle auf der Basis des Netzes in Abb. 2.4. Sobald die Anzahl der Netze und Router anwächst, wird die erfolgreiche Routenwahl jedoch zunehmend komplexer und die Pflege der Routing-Tabellen sehr aufwendig. Moderne Router aktualisieren daher die Routing-Tabellen dynamisch mit Hilfe von Routenwahlprotokollen. Hierbei tauschen sie Informationen zu den verbundenen Netzen, den verfügbaren Routen und deren Leistungsfähigkeit aus, wobei letzteres anhand von Kriterien wie Entfernung, Durchsatz, Fehlerrate und Kosten der Verbindung bewertet wird. Leistungsfähige Routenwahlprotokolle spüren veränderte Bedingungen der verbundenen Netze schnell auf und aktualisieren die Routing-Tabellen entsprechend, ohne jedoch durch diesen Informationsaustausch die Netzkapazität, die ja primär der Übermittlung von Anwenderdaten dienen soll, gravierend zu beeinträchtigen.

Beispiel:

Ein Netz mit vier Systemen basierend auf Abb. 2.4. Jedes dieser Systeme hat eine eigene Routing-Tabelle mit jeweils drei Einträgen. Diese vier, eigentlich getrennten Tabellen zeigt Tab. 5. Für jede Route ist dort das System angegeben, das direkt als Router erreichbar ist.

System	Ziel	Router
A	194.34.1	194.34.1.1
A	194.34.2	194.34.1.2
A	194.34.3	194.34.3.1
B	194.34.1	194.34.1.2
B	194.34.2	194.34.2.1
B	194.34.3	194.34.1.1
C	194.34.1	194.34.2.1
C	194.34.2	194.34.2.2
C	194.34.3	194.34.2.1
D	194.34.1	194.34.3.1
D	194.34.2	194.34.3.1
D	194.34.3	194.34.3.2

Tab. 5: Routing-Tabelle

Kann ein System (C und D) nur genau ein anderes System direkt erreichen, das als Router fungieren kann, so ist es am einfachsten in seiner Routing-Tabelle lediglich einen Eintrag mit dem Ziel Null und dem entsprechenden

Router zu machen. Dies bedeutet, daß alles zu diesem Router geschickt wird, für das kein direkter Pfad bekannt ist.

2.5 Point-to-Point Protocol (PPP)

PPP gehört zur Internet-Protokollfamilie und wird benutzt, um Datenblöcke über serielle Punkt-zu-Punkt-Verbindungen (z.B. Telefonleitungen) zu übertragen. Dadurch wird es u.a. möglich PC-basierende Endsysteme über ISDN an private Netze (WAN) und an das Internet anzubinden. Die wichtigsten Merkmale von PPP sind:

- Multiprotokollfähigkeit
Über eine Leitung können Pakete nach unterschiedlichen Netzprotokollen (IP, IPX, ...) übertragen werden
- PPP versucht Interoperabilität zwischen zwei Endgeräten zu realisieren, indem beim Verbindungsaufbau in einer Verhandlungsphase Konfigurationsdaten der beiden Endgeräte ausgetauscht werden (z.B. maximale Datenblocklänge, Kompressionsverfahren, ...)
- Authentisierung
Mit Hilfe von Benutzererkennung und Kennwort kann sich der Rechner am entfernten Ende authentisieren. Dazu werden die Protokolle PAP (Password Authentication Protocol) und CHAP (Challenge Handshake Authentication Protocol) eingesetzt
- IP-Adreßvergabe
Beim Verbindungsaufbau kann einer Gegenstelle eine IP-Adresse zugewiesen werden. Damit kann mit einer limitierten Anzahl von IP-Adressen vielen Stationen, wenn auch nicht allen gleichzeitig, der Zugang zu einem Netz ermöglicht werden
- Multi Link PPP
Durch Aufteilung des Datenstroms auf mehrere PPP-Verbindungen kann die Bandbreite erhöht werden, wenn große Datenmengen übertragen werden müssen.

2.6 Network Address Translation (NAT)

Ausgehend von einem internen Netzwerk (LAN) und einer weiteren Verbindung des Routers zu einem externen Netzwerk (WAN) wird die Umsetzung von Netzwerkadressen beschrieben. Die Verbindung zum WAN wird über ein Transportmedium (ISDN, PPPoE) hergestellt und im Folgenden als Transportverbindung bezeichnet. Eine Verbindung über IP wird Netzwerkverbindung genannt. Man unterscheidet zunächst zwei Arten von Umsetzungen bei Netzwerkverbindungen, genauer Umsetzungsrichtungen: Vom LAN zum WAN und umgekehrt von WAN ins LAN. Weiterhin muß differenziert werden, um welches Protokoll es sich handelt, da es nicht ausreichend ist, nur die IP-Schicht zu betrachten. Z. Zt. wird nur NAT für TCP und UDP unterstützt. Wenn von Adressen gesprochen wird, ist immer das Paar aus IP-Nummer und Port-Nummer gemeint. Oberhalb der Protokolle TCP bzw. UDP gibt es weitere Protokollschichten, die ebenfalls von der Umsetzung betroffen sind. Hierbei ist als bekanntester Vertreter FTP zu nennen. Der Einsatz von NAT bringt an Vorteilen:

- * Die im LAN befindlichen Rechner sind aus dem WAN nicht direkt sichtbar und damit auch nicht direkt angreifbar (Sicherheitsaspekt)
- * Sie können einem beliebigen IP Nummernkreis angehören.

2.6.1 LAN zu WAN

Bei der wohl am häufigsten gebrauchten Richtung nimmt der Router ein Paket vom LAN, ersetzt die ursprüngliche Absenderadresse durch seine eigene und transportiert das so veränderte Paket ins WAN. Da die Zieladresse unverändert bleibt, wird das Paket zum ursprünglichen Ziel geroutet und löst dort ggf. eine Antwort aus. Diese Antwort trägt natürlich als Zieladresse die vom Router eingesetzte IP-Adresse und Port-Nummer. Beim Router angelangt, erkennt dieser das Paket als eine Antwort auf das gesendete Paket und ersetzt nun die Zieladresse durch die ursprüngliche Absenderadresse in seinem dahinter liegenden WAN. Aus Sicht des Rechners, der die Verbindung initiiert hat und ein Paket ins WAN geschickt hat, sieht die Antwort aus, als hätte er direkte Verbindung zum WAN. Aus

Sicht des Zielrechners im WAN sieht das Paket aus, als wäre es vom Router gekommen.

2.6.2 WAN zu LAN

Diese Richtung wird weniger häufig genutzt und ist bei einigen Routern nicht konfigurierbar. Ein Rechner im WAN möchte eine Verbindung zu einem Rechner im LAN herstellen. Da aus Sicht des WAN nur der Router mit seiner IP existiert, muß also im Router selbst eine Zuordnung zwischen dem Paket aus dem WAN und i.A. genau einem Rechner aus dem LAN getroffen werden. Dies wird bei den Port orientierten Protokollen TCP und UDP dadurch erreicht, daß ein spezieller Port des Routers für eine Weiterleitung zu genau einem Rechner und einem Port dort konfiguriert wird. Diese Umsetzung wird als „Reverse NAT“, statisches NAT oder Port Forwarding bezeichnet. Im Zusammenhang mit dynamischer IP Vergabe ist diese Art der Umsetzung nur begrenzt einsetzbar, da die IP Adresse des angebotenen Dienstes (Ports) sich bei jeder neuen Transportverbindung ändern kann und damit aus dem WAN nicht erkennbar ist, unter welcher IP Adresse sich diesmal der Router befindet. Dies kann nur durch Anmeldung bei einem zentralen Verzeichnisdienst behoben werden.

2.6.3 Verbindungsüberwachung

Die Richtung einer Netzwerk-Verbindung wird durch das erste Paket bei UDP bzw. durch den Verbindungsaufbau (SYN) bei TCP festgelegt. Der Router hat im LAN eine feste aber variabel konfigurierbare Netzwerkadresse. Über diese werden alle Pakete vom und zum LAN transportiert. WAN-seitig kann entweder ebenfalls eine feste aber variabel konfigurierbare Adresse existieren oder aber dynamisch beim Verbindungsaufbau zur WAN-Gegenstelle via PPP eine solche IP für diese Verbindung zugeteilt werden. I.A. wird wieder bei einer neuen Transport-Verbindung auch eine andere IP zugeteilt. Der Router selbst verwaltet für seine WAN-seitige IP bei den Protokollen TCP und UDP getrennt ab der Nummer 1024 die Portnummern. Eine LAN-seitig initiierte Verbindung bekommt einen Port auf der WAN Seite zugewiesen und behält diesen für die Dauer der Verbindung (TCP) oder im Falle des verbindungslosen Protokolls UDP für eine bestimmte Zeitdauer. Aus Sicherheitsgründen existiert eine solche Zeitschranke auch für TCP, damit unbenutzte, aber nicht oder nicht korrekt beendete Verbindungen gekappt werden und nicht aus dem WAN für mögliche Angriffe zur Verfügung stehen. Aus diesen Gründen sollte die Zeitschranke auf einem möglichst kleinen Wert stehen. Da der Router eine Liste der verwendeten Ports führt, kann er leicht eine Zuordnung zu den einzelnen Verbindungen/Paketen treffen. Nach dem Abbau einer Transportverbindung und einem anschließenden Neuaufbau mit einer anderen IP wird die alte Zuordnungstabelle gelöscht, da die alten Pakete aus dem WAN den Router wegen der neu zugeteilten Adresse nun nicht mehr erreichen können. Im Falle einer TCP Verbindung signalisiert der Router dies dem LAN-Rechner durch ein TCP-RST-Paket, was diesen i.A. zu einem Neuaufbau der TCP-Verbindung veranlaßt.

3 Installation

3.1 Benötigte Informationen

Bevor Sie beginnen, sollten Sie folgende Fragen geklärt haben:

- welche IP-Adresse soll dem Router zugewiesen werden?
- welche Netzmaske hat Ihr LAN-Segment?

Zumindest diese Informationen werden benötigt, um den Router so voreinzustellen, daß nach Anschluß an das LAN eine weitergehende Konfiguration über einen Web-Browser möglich wird.

Für die spätere Konfiguration werden weitere Informationen benötigt, wie z.B.

- wird für abgehende ISDN-Rufe eine Amtsholziffer benötigt, wenn ja welche ?
- auf welche Rufnummer (MSN) soll der Router bei eingehenden Rufen reagieren ? Falls andere Geräte mit dem Router am selben Bus betrieben werden sollten die MSNs eindeutig sein !

3.2 Voraussetzungen zum Anschluß von HERMES-PRO/X

Die Telekom unterscheidet bei S0-Anschlüssen den sogenannten Mehrgeräteanschluss vom Anlagenanschluss. Am NTBA eines Mehrgeräteanschlusses kann ein Bus installiert werden, an dem sich mehrere ISDN-Geräte anschließen lassen. Der Anlagenanschluss ist für den Betrieb von (durchwahlfähigen) TK-Anlagen vorgesehen. An einen Anlagenanschluss darf nur ein Gerät (die Anlage) angeschlossen werden. HERMES-PRO/X wird an einem **DSS-1** (Euro-ISDN) **S0 Mehrgeräte**-Anschluss betrieben. Der Betrieb an einem Anlagenanschluss ist möglich, jedoch nicht empfehlenswert/sinnvoll, da kein weiteres Gerät, d.h. keine Anlage angeschlossen werden kann. Welche Form des Anschlusses vorliegt, muß jeweils vor Ort geklärt werden ! Im folgenden werden verschiedene Anschlusskonfigurationen näher beschrieben:

1) Mehrgeräteanschluss mit S0-Bus

HERMES-PRO/X kann am S0-Bus oder auch direkt am NTBA (freie Buchse) angeschlossen werden.

2) Mehrgeräteanschluss mit TK-Anlage zur a/b Umsetzung

Consumer TK-Anlagen besitzen intern oft nur a/b Schnittstellen zum Anschluss analoger Endgeräte. Derartige Anlagen sind direkt am NTBA oder an einem installierten S0-Bus angeschlossen; die Auswahl der Endgeräte erfolgt beim Mehrgeräteanschluss über die MSNs. HERMES-PRO/X wird *neben* der Anlage, wie bei 1) am S0-Bus oder auch direkt am NTBA (freie Buchse) angeschlossen. Die Anlage muss so konfiguriert werden, daß sie nicht mit HERMES um Rufe konkurriert (disjunkte MSNs!).

3) TK-Anlage mit internen S0-Anschlüssen

HERMES-PRO/X sollte an einen internen S0-Bus der TK-Anlage angeschlossen werden, da die bei 2) beschriebene Konfigurationsproblematik dann entfällt. Ist das NTBA wie bei 2) als Mehrgeräteanschluss konfiguriert, so kann HERMES-PRO/X auch wie unter 2) beschrieben angeschlossen werden.

3.3 Aufstellen und Anschließen

Ihr Router HERMES-PRO/X muß an einem trockenen, sauberen und gut belüfteten Ort aufgestellt werden. Das Gerät enthält keinen Lüfter, der ausfallen könnte, dafür muß aber die Luftzirkulation insbesondere an den Be- und Entlüftungsschlitzen gewährleistet sein!

Gehen Sie beim Anschließen in der folgenden Reihenfolge vor:

1. An der Rückseite des Gerätes befinden sich fünf RJ45-Buchsen mit Ethernet-Schnittstellen, welche mit *P2* bis *P6* beschriftet sind. Schließen Sie eine der Buchsen mit dem beiliegenden roten Kabel an die Netzwerkkarte Ihres Rechners an.
2. Verbinden Sie den Port *P1* mit Ihrem DSL-Modem oder Ihrem IP-Gateway.
3. Verbinden Sie die *S0*-Schnittstelle auf der Geräterückseite mit dem mitgelieferten gelben ISDN-Kabel mit ihrer ISDN-Dose.
4. Schliessen sie da Kabel des mitgelieferten Steckernetzteils in die mit *DC* beschriftete Buchse des Routers an. Dann können Sie das Steckernetzteil in eine 220 Volt Steckdose stecken.

Sobald Sie den schwarzen EIN/AUS-Taster an der Frontseite drücken, startet das Betriebssystem des Routers. Sie erkennen den Startvorgang an dem Lauflicht der linken Vierergruppe gelber Leuchtdioden an der Frontseite. Haben Sie alles wie oben beschrieben angeschlossen, leuchtet die *S0*- und eine der grünen *LINK*-Leuchtdioden, sobald das Betriebssystem bereit ist.

3.4 Bedeutung der LED Anzeigen

Auf der Frontplatte von HERMES-PRO/X befinden sich mehrere Gruppen von LEDs, deren Bedeutung in der folgenden Tabelle erklärt ist:

LED	Farbe	Bedeutung
S0	Gelb	Aktivierung der physik. Schicht des S0 Anschlusses.
D	Gelb	Aktivität im ISDN D-Kanal (Vermittlungskanal).
B1	Gelb	Der ISDN B1-Kanal ist durchgeschaltet.
B2	Gelb	Der ISDN B2-Kanal ist durchgeschaltet.
ST	Gelb	Reserviert
SY	Gelb	Reserviert
TX	Gelb	Reserviert
RX	Gelb	Reserviert
LINK/RCV <i>n</i>	Grün	Aktivierung der physischen Schicht des Ethernet Ports N. Diese LED leuchtet, wenn zwei Ethernet-schnittstellen korrekt miteinander verbunden sind. Sie blinkt bei Aktivität auf dem Port.
SPEED 100 <i>n</i>	Gelb	Port läuft mit 100 MBit.

Tab. 1: LED Anzeigen

Wenn die LEDs *S0*, *D*, *B1* und *B2* blinken, dann ist HERMES-PRO/X dabei das Betriebssystem zu laden.

3.5 Erste Schritte

Die IP-Schnittstellen von HERMES-PRO/X sind bei der Auslieferung auf folgende Werte gestellt:

Schnittstelle	IP Adresse	Netzmaske
Ethernet	192.168.1.254	255.255.255.0
ISDN mif0	192.168.3.1	
Routerprozeß isdnd	192.168.4.1	

Tab. 2: IP Adressen

Die voreingestellten IP Adressen sind Intranet IP Adressen, die im Internet nicht vorkommen dürfen. Sollten Sie in Ihrem LAN bereits die Ethernet-Adresse 192.168.1.254 vergeben haben, dann sollten sie HERMES-PRO/X nicht an Ihr LAN anschließen, solange Sie die IP-Adresse nicht geändert haben.

Die Konfigurationsoberfläche des Routers sollte jetzt mit Ihrem Web-Browser über folgende Adresse erreichbar sein:

<http://192.168.1.254:7705/>

Geben Sie als Benutzernamen

root

ein. Das Kennwort, welches bei der Auslieferung eingestellt ist heisst:

HERMES

Nachdem Sie Konfigurationsänderungen über einen Web-Browser vorgenommen haben, vergessen Sie nicht die Änderungen persistent zu machen, indem Sie folgende Menüpunkte auswählen:

Save configuration to files

und dann

Write files to Flash ROM.

Falls das Kennwort geändert wurde und nicht mehr bekannt ist, oder die IP Adresse geändert wurde und nicht mehr bekannt ist, dann lesen Sie bitte im entsprechende Kapitel im Anhang unter Troubleshooting nach.

4 Ethernet-Switch

4.1 Beschreibung der Funktionseinheit

In HERMES-PRO/X ist ein Switch mit fünf gleichwertigen Ethernet Ports (P2 bis P6) integriert, an dem die LAN-Geräte angeschlossen werden. Zusätzlich stellt der Port P1 einen weiteren Ethernet Anschluss dar, über welchen ein DSL Modem oder ein externes Gateway angeschlossen werden kann.

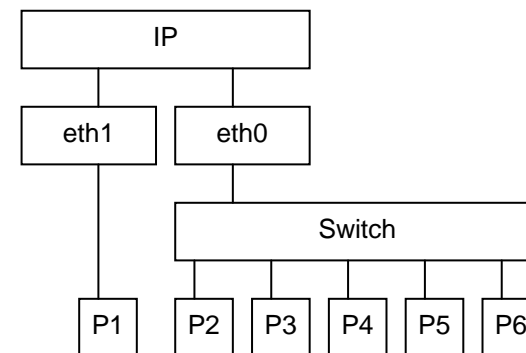


Abb. 4.1: Switch

An allen Ports ist eine automatische Crossover Funktion integriert, d. h. beim Anschluß von Rechnern oder weiteren Switchs bzw. Hubs zwecks Porterweiterung muß nicht darauf geachtet werden, daß das Ethernet-Kabel gedreht oder nicht-gedreht ist.

Der Switch beinhaltet Quality of Service Funktionen, d.h. bestimmte Pakete können bevorzugt behandelt werden. Dabei werden die folgenden Klassifikationen eingesetzt:

- IEEE 802.3ac Tag mit IEEE 802.1p Prioritätsinformation
- IPv4 Type of Service (TOS) Feld

5 USB Schnittstelle

In HERMES-PRO/X ist eine USB Host Schnittstelle eingebaut. An diese Schnittstelle können prinzipiell verschiedene USB Geräte angeschlossen werden. Zur Zeit werden jedoch lediglich Memory Sticks (Memory Devices) unterstützt.

Es gibt zwei Anwendungsfälle, bei denen Memory Sticks eingesetzt werden können.

5.1 Start mit spezieller Konfiguration

Es ist möglich den Router zu starten, so dass die Konfigurationsdateien von einem Memory Stick verwendet werden. Dazu muss der Memory Stick beim Startvorgang an den Router angeschlossen sein. Der Memory Stick muss ein VFAT Dateisystem und die Verzeichnisse `\etc` und `\usr\lib\hermes` enthalten. Das VFAT Dateisystem ist der Standard unter Windows.

Wenn der Router beim Start einen Memory Stick erkennt, dann kopiert er **alle** Dateien aus den Verzeichnissen `\etc` und `\usr\lib\hermes` in das Dateisystem des Routers, anstatt die Dateien aus dem eingebauten Flashspeicher zu kopieren. Somit verwendet der Router die Konfiguration, welche im Memory Stick gespeichert ist.

Wenn beim Zugriff auf den Memory Stick ein Fehler auftritt, dann verwendet der Router die Konfigurationsdateien aus dem eingebauten Flashspeicher.

Folgende Dateien sollten mindestens auf dem Memory Stick enthalten sein:

```
\etc\hosts
\etc\ihosts
\etc\passwd
\usr\lib\hermes\isdnd.cfg
```

Für Testzwecke können Sie auch weitere Startup Skripte verwenden, welche Sie selber erstellen oder von MULTIDATA geliefert bekommen, wie z. B.:

```
\etc\s09route (zusätzlich statische Routen)  
\etc\s40watchdog (Überprüfung auf abgestürzte Programme)
```

Ausserdem können Zertifikate auf den Router übertragen werden.

5.2 Verwendung zur Laufzeit

Sie können den Memory Stick auch zur Laufzeit an den Router anschließen, um ihn dann als zusätzlichen Datenträger zu verwenden. Dazu müssen Sie sich per telnet beim Router anmelden und folgenden Befehl ausführen:

```
# mount /dev/sda1 /mnt
```

Der Datenträger steht danach im Verzeichnis `/mnt` zur Verfügung. Sie können dann Dateien von und zu dem Datenträger kopieren oder direkt auf dem Datenträger ausführen.

Bevor Sie den Memory Stick entfernen, müssen Sie folgenden Befehl ausführen, damit das Betriebssystem alle ausstehenden Schreiboperationen abschließt:

```
# umount /dev/sda1
```

6 Routerfunktion

6.1 Struktur

HERMES-PRO/X liegt ein UNIX Betriebssystem zugrunde. Die Basis der Routerfunktion ist der schon erwähnte Softwarerouter HERMES-IP. Die Implementierung besteht im wesentlichen aus drei Teilen:

- der IP-Schnittstelle *mif*
- dem Benutzerprozeß *isdnd*
- dem CAPI-Treiber *capi20*.

Die Abhängigkeiten zwischen den einzelnen Funktionsmodulen sind dabei in der folgenden Abbildung dargestellt.

6.2 Die IP-Schnittstelle

Die Schnittstelle zum TCP/IP Protokoll-Stack bildet der *mif* Treiber, der sich als Netzwerkschnittstelle *mif0* darstellt. Alle IP-Pakete werden transparent zu dem Benutzerprozeß *isdnd* durchgereicht. Das Vorhandensein der Netzwerkschnittstelle zeigt der Befehle:

```
ifconfig mif0
mif0: flags=8d1<UP,POINTOPOINT,RUNNING,NOARP,SIMPLEX>
      inet 192.168.3.1 --> 192.168.4.1 netmask fffffff0
```

6.3 Der Routing-Prozeß

Der Hauptteil besteht aus dem Hintergrundprozeß *isdnd*, der die zur Verfügung stehenden ISDN-Kanäle verwaltet und die Zuordnung von IP-Paket zu WAN Schnittstelle trifft.

isdnd kann als eigenständiger IP-Knoten angesehen werden. Deswegen gibt es auch eine eigene IP-Nummer für *isdnd*. Dieser Knoten hat genau eine Verbindung zum Host-Rechner. Die Schnittstelle, die diese Verbindung bedienen kann, wird auf der Host-Seite durch den *ifconfig* Befehl als *mif0* bekannt gemacht. Die Verbindung wird von *mif* als Punkt-zu-Punkt-Verbindung (Point-To-Point) klassifiziert (nicht zu verwechseln mit PPP).

Durch die Punkt-zu-Punkt-Konfiguration ist gewährleistet, daß sporadische IP-Pakete, wie sie z.B. auf einem Ethernet für Routenwahlinformationen übertragen werden, nicht auftreten.

Der TCP/IP Knoten *isdnd* verwaltet beliebig viele Verbindungen zu weiteren Knoten, die über ISDN zu erreichen sind. Die Zuordnung zwischen Telefonnummer und IP-Nummer geschieht mit Hilfe einer Routing-Tabelle. *isdnd* selbst reicht alle IP-Pakete transparent durch, mit Ausnahme des Feldes *TTL* (time to live), das um eins vermindert wird. Falls dieses Feld den Wert 0 erreicht, dann wird das Paket verworfen. An die eigene Adresse gerichtete Pakete werden zur Zeit ebenfalls verworfen.

6.4 Datenübertragung

isdnd empfängt von der *mif*-Schnittstelle IP-Pakete und ermittelt anhand der IP-Zieladresse, welcher B-Kanal zu dem Zielrechner führt. Falls noch keine Verbindung besteht, wird das Paket erst übertragen, nachdem eine Verbindung aufgebaut wurde.

Bei ankommenden Rufen wird eine Verbindung aufgebaut, und die danach ankommenden IP-Pakete werden der *mif*-Schnittstelle übergeben.

6.5 Verbindungsabbau

Ein Abbau der WAN Verbindung findet statt, wenn in einer konfigurierbaren Zeitspanne keine IP-Pakete übertragen werden. Diese Zeitspanne ist durch einen Konfigurationsparameter sowohl global als auch für jede Gegenstelle einstellbar. Durch die Konfiguration der *mif*-Schnittstelle ist gewährleistet, daß sporadische IP-Pakete, wie sie z.B. in einem LAN für Routinginformationen übertragen werden, nicht auftreten. Falls aus anderen Gründen sporadisch unerwünschte IP-Pakete über eine WAN Verbindung geschickt werden, z.B. beim Einsatz von Netbios Anwendungen von Microsoft Betriebssystemen, dann müssen diese Pakete über den Firewall-Mechanismus herausgefiltert werden (siehe Kapitel 7).

6.6 Routing

Die Zuordnung von IP-Adresse zu Gegenstellen im WAN geschieht in der Datei */etc/hosts*. Das Format der Datei entspricht dem üblichen UNIX-Dateiformat für Systemdateien (vgl. */etc/hosts*). Eine Zeile enthält entweder zwei oder fünf Spalten. Die erste Spalte enthält immer die IP-Nummer der Gegenstelle. Anstatt von IP-Nummern können auch symbolische Namen verwendet werden.

```
# ihosts ISDN Hosts Beschreibung. MULTIDATA GmbH
# IP      CALL/Section  LISTEN      L2    L3
192.68.3.5 00615197672  0615197672  0     0
ppphost   pppSection
```

Abb. 6.1: Beispiel der Datei *etc/hosts*

Besteht eine Zeile aus zwei Spalten, dann verweist die zweite Spalte auf einen Abschnittsnamen in der Datei */usr/lib/hermes/isdnd.cfg*.

Eine Gegenstelle mit Standardparametern kann auch komplett in einer Zeile definiert werden, wenn fünf Spalten angegeben werden. *CALL* gibt die zu rufende ISDN-Nummer an. *LISTEN* gibt die ISDN-Nummer an, auf die bei einem ankommenden Ruf verglichen wird. Die Unterscheidung zwischen *CALL* und *LISTEN* ist z.B. durch die Amtsholung bei einer Telefonnebenstellenanlage erforderlich. Das Schicht 2 und Schicht 3 Protokoll kann für jede Gegenstelle angegeben werden und wird entsprechend der CAPI-Spezifikation kodiert.

Es findet kein dynamisches Routing statt. Änderungen und Erweiterungen der Routingtabelle müssen manuell durchgeführt werden (statisches Routing). Es werden keine Informationen über die *isdnd*-interne Routing-Tabelle an andere Rechner weitergegeben. Insbesondere werden keine Routing-Pakete (RIP) ausgewertet.

Eine Telefonnummer kann für mehrere IP-Adressen (oder ein Netz) zuständig sein! Falls ein B-Kanal zu einer solchen Telefonnummer aufgebaut ist, werden alle IP-Pakete, die zu Rechnern, die über diese Telefonnummer zu erreichen sind über den bestehenden B-Kanal geschickt. Es ist kein zweiter Verbindungsaufbau nötig.

6.7 Besondere Adressen

Die IP Adresse *0.0.0.0* kann als Standardroute für abgehende Rufe verwendet werden. Ein Stern (*) in der Spalte *LISTEN* kann als Standardverbindung für eingehende Rufe verwendet werden.

6.8 ISDN Schicht 2 und Schicht 3 Protokolle

Prinzipiell kann jede Nummer für die Schicht 2 und Schicht 3 Protokolle angegeben werden. Diese Nummern werden in entsprechende CAPI-Nachrichten eingetragen. Die von der CAPI-Implementierung unterstützten Protokolle können mit dem Befehl

```
hcmd -p
```

in Erfahrung gebracht werden. Die zur Zeit von HERMES-PRO/X unterstützten Protokolle sind im Anhang B.2 Tabelle der B-Protokolle aufgelistet.

Als Schicht 2 Protokoll wird Transparent HDLC empfohlen. Das Protokoll X.75 realisiert unter anderem eine Datensicherung, die für TCP/IP nicht zwingend notwendig ist.

Als Schicht 3 Protokoll wird Transparent empfohlen.

Falls die eingestellten Protokolle von zwei Kommunikationspartnern unterschiedlich sind, kommt in der Regel eine Verbindung zustande, es können jedoch keine Daten ausgetauscht werden.

6.9 Schutz vor Mißbrauch

Die Routing-Tabelle enthält Informationen über Telefonnummern, die zugangsberechtigt sind. Falls die Telefonnummer eines ankommenden Rufes nicht in der Routing-Tabelle vorkommt, wird der Ruf zurückgewiesen, d.h. die Verbindung wird abgebaut und es entstehen keine Gebühren. Dadurch wird der Mißbrauch des ISDN-Anschlusses und der TCP/IP-Dienste durch unbefugte Anrufer verhindert.

6.10 PPP über ISDN

HERMES-PRO/X unterstützt synchrones PPP über ISDN (RFC 1548, RFC 1618), IP Adressaushandlung (RFC 1332), die Authentisierungsverfahren

CHAP (RFC 1994) und PAP (RFC 1172) und die LCP Erweiterung für automatischen Rückruf (RFC 1570).

6.11 Callback

Der Callback Mechanismus (automatischer Rückruf) kann dazu verwendet werden die Verbindungsgebühren durch die angerufene Station übernehmen zu lassen. Folgende Parameter sind beim automatischen Rückruf relevant:

- * die Identifikation und die Authentisierung des Anrufers
- * die zurückzurufende Nummer
- * die Zeitdauer nach der zurückgerufen wird

Mit HERMES-PRO/X stehen mehrere Methoden einen automatischen Rückruf zu realisieren zur Verfügung:

- 1) Die Identifikation erfolgt durch die Signalisierung der Rufnummer des Anrufers (CLGPN) im ISDN. Der Angerufene vergleicht die CLGPN mit dem Parameter **listen** aus der Routing Tabelle (siehe Kapitel Routing). Die zurückzurufende Nummer ergibt sich aus dem zugehörigen Parameter **call**. Die Zeitdauer für den Rückruf ergibt sich aus dem Parameter **callback** im Abschnitt [Peer].

Für den Anrufer ist keine besondere Konfiguration nötig. Es fallen keine Gebühren an. Damit diese Rückrufmethode verwendet werden kann, müssen folgende Bedingungen erfüllt sein:

- * Das Dienstmerkmal CLIP ist aktiv, d.h. die Anzeige der Rufnummer wird nicht unterdrückt.
- * Der Anrufer nimmt Rufe entgegen; dies ist bei Windows Clients normalerweise nicht der Fall.

- 2) Diese Methode entspricht der PPP Callback Option, wie sie in RFC1570 definiert ist. Mit dieser Protokolloption fordert der Anrufer den Angerufenen zum Rückruf auf. Der Anrufer teilt dem Angerufenen mit, wie der Rückruf erfolgen soll. Der RFC1570 definiert die möglichen Vorgehensweisen, die im folgenden als **CallbackType** bezeichnet werden:

0 Der Anrufer wird über den PAP/CHAP Namen identifiziert und über eine Nummer zurückgerufen, die beim Angerufenen konfiguriert ist (der Parameter **call**).

1 Der Anrufer übergibt eine zurückzurufende Nummer.

- 2 Der Anrufer übergibt eine Ortsbezeichnung. Die zurückzurufende Nummer ergibt sich aus einer Tabelle, die dem Anrufenden vorliegt.
- 3 Der Anrufer übergibt eine zurückzurufende Nummer im E.164 Format.
- 4 Der Anrufer übergibt einen eindeutigen Namen über den eine Identifikation, aber keine Authentisierung stattfindet. Der Angerufene vergleicht den Namen mit dem Parameter **Peer Name** aus dem Menü *ISDN Peer Stations* der Web-Oberfläche (d.h. dem Abschnittsnamen in *isdnd.cfg*. Die zurückzurufende Nummer ergibt sich aus dem zugehörigen Parameter **Ca11**.

Als Anrufer lassen sich alle Callback Typen unter HERMES-PRO/X konfigurieren. Als angerufene Station sind nur die Typen 0 und 4 implementiert. Es wird empfohlen Callback mit einem Authentisierungsverfahren zu verbinden, d.h. **callbackType=0**. Der Rückruf bei Callback über PPP/LCP erfolgt immer nach 10 Sekunden.

- 3) Diese Methode entspricht dem Callback Control Protocol (CBCP, MS Callback) wie es von Microsoft ab Windows 95 bzw. Windows NT 4.0 verwendet wird. Zu MS Callback gibt es kein RFC, es existiert jedoch ein (inzwischen veraltetes) Internet-Draft Dokument, das über folgende Adresse zu bekommen ist: <ftp://ftp.multidata.de/pub/doc/mscbcp.txt>. CBCP wird über PPP ausgehandelt. Dabei bietet der Angerufene an, den Anrufenden über bestimmte Vorgehensweisen zurückzurufen. Der Anrufer kann sich für eine Vorgehensweise entscheiden und die damit benötigten Informationen an den Angerufenen übertragen. HERMES-PRO/X unterstützt nur die Vorgehensweise ‚Callback to a pre-specified or administrator specified number‘ als angerufene Station. Dabei wird der Anrufer über den PAP/CHAP Namen *RemoteName* identifiziert und über die für diese Gegenstelle konfigurierte Nummer zurückgerufen. Der Rückruf bei CBCP erfolgt immer nach 10 Sekunden. HERMES-PRO/X unterstützt MS Callback nicht als Anrufer.

Methode	Anrufer		Angerufener		
	[Abschnitt] Parameter	Wert	[Abschnitt] Parameter	Wert	
1)	Es wird keine spezielle Konfiguration benötigt		[Peer]		
			Callback	-1 Kein Callback ≥ 1 Sekunden bis zum Rückruf	
2)	[PeerLCP]		[PeerLCP]		
	Callback Mode	8 Outgoing	Callback Mode	4 Incoming	
	CallbackType	0 User authentication	Anrufer mit CallbackType 0 und 4 werden unterstützt		
		1 Dialing string			
		2 Location ID			
3 E.164 number					
4 Distinguished name					
CallbackID	Zeichenkette entsprechend CallbackType				
3)	Wird nicht unterstützt		[PeerLCP]		
			Callback Mode	4 Incoming	

Tab. 1: Callback Konfiguration

6.12 Kanalbündelung

Die automatische Kanalbündelung (Bandwidth On Demand, BOD) dient zur Erhöhung des Nutzdatendurchsatzes und ist in HERMES-PRO/X in einer proprietären Methode implementiert. Wenn zu einer Gegenstelle mehrere B-Kanäle aufgebaut sind, dann teilt der Routingprozeß prinzipiell die Datenpakete gleichmäßig auf die bestehenden B-Kanäle auf. Bei zwei B-Kanälen kann der Router somit einen Durchsatz von 128 kBits/s je Richtung erzielen.

Als Voreinstellung baut der Routingprozeß nur genau eine ISDN Verbindung zu einer Gegenstelle auf. Sobald die Kapazität des bestehenden B-Kanals für das Nutzdatenaufkommen nicht mehr ausreicht, baut der Routingprozeß einen weiteren B-Kanal auf. Der Parameter **MaxChan** in der Konfigurationsdatei `isdnd.cfg` legt fest, wieviele B-Kanäle der Routingprozeß maximal für eine Gegenstelle verwenden darf. Bei der Konfiguration über

einen Web-Browser setzt die Einstellung BOD=YES den Parameter **MaxChan** auf 2.

6.13 Debugging

Anhand von Debug-Ausgaben kann der Zustand von *isdnd* komfortabel überprüft werden. Dazu stehen verschiedene Klassen und Stufen von Debug-Ausgaben zur Verfügung:

1. Fehler und Warnungen:

Die Ausgabe dieser Meldungen erscheint in der Logdatei */usr/lib/hermes/isdnd.log*. Neue Meldungen werden an eine bestehende Datei angehängt. Die maximale Größe der Logdatei ist über den Parameter *LogfileSize* im Abschnitt [ISDND] der Datei *isdnd.cfg* einstellbar.

Welche Meldungen ausgegeben werden, wird durch **Ziffern** in dem Parameter *Debug* bestimmt.

2. Debug-Ausgaben:

Die Ausgabe dieser Meldungen erfolgt an die Standardfehlerausgabe (stderr), welche in der Regel in die Datei *isdnd.log* umgeleitet wird. Welche Meldungen ausgegeben werden, wird durch **Buchstaben** in dem Parameter *Debug* bestimmt.

6.14 Interoperabilität

Die Interoperabilität wurde bisher mit folgenden Fremdprodukten getestet:

- Banzai-Router
- BIANCA/BRICK-XS
- CiscoPro CPA1003/CPA1004
- ITK-Router
- netGW
- Windows 95
- Windows NT

MULTIDATA garantiert jedoch nicht für die einwandfreie Zusammenarbeit mit diesen und anderen Produkten. Bei Windows 95 ist die Konfiguration von PPP zusätzlich abhängig vom Hersteller des ISDN-Treibers und kann zu Inkompatibilitäten führen.

7 Firewall-Mechanismus

Firewalls stellen eine Methode dar, ein Netzwerk gegen Fremdeinwirkung zu schützen. Alle aus dem externen Netz eintreffenden oder von dem internen Netz ausgehenden Informationen müssen die Firewall passieren.

Eine Firewall entscheidet anhand bestimmter Kriterien, ob ein Paket durchgelassen oder verworfen wird.

In HERMES-PRO/X wird die Open Source Firewall-Implementierung IP-Tables eingesetzt. Die Konfiguration von IP-Tables erfolgt über das Benutzerkommando iptables, welches in der Routersoftware enthalten ist und auf dem Router benutzt werden kann. Die Handbuchseiten (man page) für das iptables Kommando sind in aktuellen Linux Distributionen in dem Paket iptables enthalten, welches sich in der Gruppe Anwendungen/Netzwerk befindet. In der Linuxdistribution und im Internet gibt es ebenfalls HOWTOS, die sich mit dem Thema IP-Tables und Firewall beschäftigen.

7.1 Konfigurationsmöglichkeiten

Durch die IP-Nummern bezogenen Regeln wird unterstützt, dass nur bestimmbare Rechner aus dem Intranet ins Internet kommen. Regeln für beliebige Protokolle lassen sich definieren. Zusätzlich zu TCP, UDP und ICMP lassen sich auch Regeln für z. B. AH und ESP definieren.

Über Kommandozeile oder ein rc Skript kann die ganze Mächtigkeit der IP-Tables Implementierung genutzt werden.

7.2 Arbeitsweise von IP-Tables

IP-Tables definiert den Begriff **Chains**. Chains haben einen **Namen** und enthalten eine sortierte Liste von **Regeln**. Es gibt drei vordefinierte Chains mit den Namen INPUT, OUTPUT und FORWARD. Die vordefinierten Chains enthalten zusätzlich eine **Policy**, die entweder ACCEPT oder DROP lautet.

Über das iptables Kommando lassen sich **benutzerdefinierte Chains** mit frei wählbaren Namen anlegen. Der Name einer Chain darf Buchstaben, Ziffern und Sonderzeichen enthalten, jedoch keine Leerzeichen!

Jede Regel besteht aus einer **Filterbeschreibung** und einer **Aktion** (Target).

Die Filterbeschreibung enthält Angaben über Eigenschaften von Netzwerkpaketen, wie z. B. IP-Nummern, Portnummern und Protokollnummern.

Eine Aktion hat einen **Namen** und eine **Bedeutung**. Eine Aktion ist eine **vordefinierte Aktion** oder eine **benutzerdefinierte Aktion**. Es gibt die vordefinierten Aktionen mit den Namen DROP, ACCEPT, RETURN und REJECT. Die vordefinierten Aktionen haben folgende Bedeutung:

Name der Aktion	Bedeutung
ACCEPT	lässt das Paket die Firewall passieren. Es werden keine weiteren Regeln abgearbeitet.
DROP	verwirft das Paket. Es werden keine weiteren Regeln abgearbeitet.
REJECT	verwirft das Paket und sendet eine ICMP Nachricht an den Absender. Es werden keine weiteren Regeln abgearbeitet.
RETURN	bricht die Abarbeitung der Regeln in der aktuellen Chain ab und kehrt zur aufrufenden Chain zurück. Falls es eine Regel in einer der drei vordefinierten Chains ist, wird das Paket entsprechend der Policy dieser vordefinierten Chain behandelt.

Tab. 1: Vordefinierte Aktionen

Weiterhin gibt es **benutzerdefinierte Aktionen**. Der Name einer benutzerdefinierten Aktion muss identisch zu dem Namen einer bestehenden benutzerdefinierten Chain sein. Die Bedeutung einer benutzerdefinierten Aktion ist, dass die Abarbeitung mit der ersten Regel der angegebenen benutzerdefinierten Chain fortgesetzt wird. Man kann sagen, die benutzerdefinierte Chain wird aufgerufen.

Regeln in einer Chain werden der Reihe nach auf IP-Pakete angewendet. Wenn eine Regel zutrifft, führt IP Tables die Aktion für dieses IP-Paket aus. Wenn das Ende einer Chain erreicht ist, führt IP-Tables implizit die Aktion RETURN aus.

7.3 Chains für HERMES-PRO

Die Routersoftware unterstützt die Konfiguration von IP-Tables über die Weboberfläche und die Konfigurationsdatei `isdnd.cfg`. Über die Web-oberfläche lassen sich Firewallregeln definieren, die in entsprechende `iptables` Aufrufe umgesetzt werden. Eine Regel tritt sofort nach ihrer Definition über die Weboberfläche in Kraft.

Beim Start von HERMES-PRO legt der `isdnd` Prozess einige Chains an, welche eine Umgebung definieren, die für benutzerdefinierte Chains verwendet wird. Das Kommando `iptables -L` bzw. `iptables -L -v` zeigt die definierten Regeln an.

In den Standardchains INPUT, OUTPUT und FORWARD legt `isdnd` Regeln an, die auf alle Pakete zutreffen, welche von oder zu der `mif`-Schnittstelle gehen. Diese Regeln enthalten als Aktion einen Sprung zu der Chain `isdnd-fw`, welche dazu dient, Sprünge zu den benutzerdefinierten Chains aufzunehmen. Pakete, welche nur die LAN Schnittstelle betreffen, insbesondere Pakete an die Ports 7703 (`vcapi`) und 7705 (Konfiguration), werden immer durch die Firewall durchgelassen.

Die Chain `isdnd-std` wird von `isdnd-fw` als erstes angesprungen. Diese Chain bewirkt, dass

1. alle Pakete, die ungültige IP-Header enthalten, verworfen werden
2. alle Pakete, die zu keiner bekannten Verbindung gehören, verworfen werden.
3. alle Pakete, die zu einer bereits aufgebauten TCP bzw. UDP Verbindung gehören, die Firewall passieren.

Für die benutzerdefinierten Chains generiert `isdnd` einen eigenen Namensraum, der immer mit der Zeichenkette `isdnd-fw:` beginnt (Sonderzeichen, wie z. B. "-" oder ":" werden von `iptables` als normale Buchstaben behandelt). Der Abschnittsname aus der Benutzerkonfiguration folgt dieser Zeichenkette. Abschliessend enthält der Chainname einen Unterstrich und eine dreistellige Nummer, die die Tabellenzeile aus der Benutzerkonfiguration angibt:

```
isdnd-fw:Abschnittname_NNN
```

Wenn der Benutzer eine vordefinierte Aktion (s. o.) für eine Regel auswählt, fügt isdnd zusätzliche Regeln ein, die folgendes bewirken:

Auswahl DROP: Auf dem Router wird zusätzlich ein Eintrag in der Datei isdnd.log gemacht, wenn Debug 6 aktiv ist. Dies entspricht der Standardeinstellung.

Auswahl REJECT: Auf dem Router wird zusätzlich ein Eintrag in der Datei isdnd.log gemacht, wenn Debug 6 aktiv ist. Dies entspricht der Standardeinstellung.

Auswahl ACCEPT: Auf dem Router wird zusätzlich ein Eintrag in der Datei isdnd.log gemacht, wenn Debug Z aktiv ist. Diese Einstellung kann zur Fehlersuche verwendet werden.

7.4 Die Stationen eines Pakets

Die Struktur der Chains bewirkt, dass ein Paket von einer Standard-Chain (INPUT, OUTPUT, FORWARD) zu der Chain isdnd-fw springt. Von dort geht es zu den Standardregeln (isdnd-std). Wenn das Paket dort nicht gepasst hat, kommt es zur isdnd-fw Chain zurück. Dann kommt das Paket zu der benutzerdefinierten Chain, welche dem Peer zugeordnet ist, zu welchem das Paket von isdnd geroutet werden soll. Dort geschieht die Verteilung auf die Chains, die die einzelnen Tabellenzeilen repräsentieren, welche der Reihe nach abgearbeitet werden. Falls keine Tabellenzeile passt, kommt das Paket zurück zu isdnd-fw Chain. Von dort geht es zur nächsten Chain in der Reihe. Diese Chain gehört jedoch zu einer anderen Peer Station. Dies ist in der Regel nicht gewünscht, wie bereits oben beschrieben. Falls keine Regel der Abschnitts-Chains passt, tritt die Policy in Kraft.

```
FORWARD -> isdnd-fw -> isdnd-std
          isdnd-fw -> isdnd-fw:AbschnittA -> isdnd-fw:AbschnittA_001
                                           isdnd-fw:AbschnittA_002
                                           ...
                                           isdnd-fw:AbschnittB -> isdnd-fw:AbschnittB_001
                                           isdnd-fw:AbschnittB_002

policy (SYSTEM Abschnitt)
```

7.5 Konfigurationsmenüs

In der Peertabelle wurde die alte Access-Spalte durch die Spalte IP-Table ersetzt:

Peer Name	IP Address	Netmask	Telno Call	Telno Signaled	L2	L3	Idle	Use NAT	BOD	Call-back	IP-Table	PPP Section
arcor	0.0.0.0	0.0.0.0	0192070	-	5	0	120	Yes	No	-1	FWinternet	PPParcor
partner	192.168.10.0	255.255.255.0	023361	23361	0	0	60	No	Yes	-1	FWpartner	PPPpartner
service	192.169.129.1	255.255.255.255	00981123	0981123	5	0	-1	No	No	-1	FWservice	PPPdefault

7.5.1 IP Tables (Firewall)

Dieses Menü erlaubt benutzerdefinierte Chains hinzuzufügen, zu ändern und zu löschen. Die HERMES-PRO spezifische Chain mit dem Namen SYSTEM ist immer vorhanden und kann nicht gelöscht werden. Eine benutzerdefinierte Chain darf nur gelöscht werden, wenn es keine Verweise aus der Peer Tabelle auf diese Chain gibt, damit keine inkonsistenten Zustände entstehen.

Section Name	Description		
FWinternet	Zugang zum Internetzugang	edit	delete
FWpartner	Zugang zur Partnerapotheke	edit	delete
FWservice	Zugang für Fernwartung	edit	delete
SYSTEM		edit	

7.5.2 New IP Tables Set

Das folgende Menü erscheint bei Betätigung des new Links im Menü IP Tables (Firewall).

Section Name:
 Description (optional):

Section Name

In diesem Menü muss zwingend ein Name für die IP Chain im Feld Section Name angegeben werden. Aus diesem Namen wird ein Name entsprechend der Beschreibung im Kapitel 7.3 generiert.

Description

Die Beschreibung der IP Chain ist optional und hat keine Auswirkung auf die Konfiguration von IP Tables. Die Beschreibung wird jedoch in der Konfigurationsdatei abgespeichert.

7.5.3 Edit IP Tables Set

Das folgende Menü erscheint bei Betätigung des edit Links im Menü IP Tables (Firewall) bei einer neu angelegten Chain. Die Tabellenzeile, die auf alle Pakete passt und als Aktion den Wert RETURN hat, erscheint immer und ist weder editierbar noch löschtbar. Diese Zeile repräsentiert das Standardverhalten von IP Tables für benutzerdefinierte Chains.

Section Name:

FWService

 Description (optional):

Zugang für Fernwartung

Source IP	Source Mask	Destination IP	Destination Mask	TCP Ports	UDP Ports	Protocols	Target	Description
0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	Any	Any	Any	RETURN	<u>insert before</u>

Bei Betätigung des Links insert before kann eine neue Tabellenzeile angelegt werden. Die Reihenfolge der Tabellenzeilen entspricht der Reihenfolge, in der IP Tables die Regeln abarbeitet und ist somit relevant für die Funktion der Firewall.

In die Tabelle mit dem Namen SYSTEM kann keine Regel eingefügt werden. Jedoch lässt sich die Standardaktion (Target) für SYSTEM als DROP oder als ACCEPT bestimmen. Damit kann das Standardverhalten der benutzerdefinierten Chains bestimmt werden.

Source IP

Beschreibung: IP-Nummer der Quelle. Dieser Wert ist in Punktschreibweise oder als DNS Name anzugeben. In Verbindung mit **Source Mask** beschreibt dieser Wert den IP-Nummernkreis des Ursprungs der Pakete, für welche diese Regel definiert ist.

Beispiel: 192.168.1.0

Standardeinstellung: 0.0.0.0

Source Mask

Beschreibung: Netzmaske der Quelle. Dieser Wert ist in Punktschreibweise anzugeben.

Beispiel: 255.255.255.0

Standardeinstellung: 255.255.255.255.

Destination IP

Beschreibung: IP-Nummer des Ziels. Dieser Wert ist in Punktschreibweise oder als DNS Name anzugeben. In Verbindung mit **Destination Mask** beschreibt dieser Wert den IP-Nummernkreis des Ziels der Pakete, für welche diese Regel definiert ist.

Beispiel: 192.168.129.0

Standardeinstellung: 0.0.0.0

Destination Mask

Netzmaske des Ziels. Dieser Wert ist in Punktschreibweise anzugeben.

Beispiel: 255.255.255.0

Standardeinstellung: 255.255.255.255.

TCP Ports

Die Portdefinition beschreibt einen oder mehrere TCP Ports, für welche diese Regel definiert ist. Die Schreibweise, wie mehrere Ports zu definieren sind, ist im Kapitel 7.7 Portdefinition beschrieben. Das Schlüsselwort **any** bezeichnet beliebige TCP Ports. Das Schlüsselwort **all** bezeichnet alle TCP Ports.

Beispiel: telnet

Standardeinstellung: any

UDP Ports

Die Portdefinition beschreibt einen oder mehrere UDP Ports, für welche diese Regel definiert ist. Die Schreibweise, wie mehrere Ports zu definieren sind, ist im Kapitel 7.7 Portdefinition beschrieben. Das Schlüsselwort **any** bezeichnet beliebige UDP Ports. Das Schlüsselwort **all** bezeichnet alle UDP Ports.

Beispiel: netbios-ns

Standardeinstellung: any

Protocols

Die Protokolldefinition beschreibt ein oder mehrere Protokolle (TCP, UDP, ICMP, ESP, ...), für welche diese Regel definiert ist. Die Protokolldefinition any bezeichnet beliebige Protokolle.

Beispiel: ESP

Standardeinstellung: any

Target

Dieser Parameter bestimmt die Aktion und somit was mit dem IP Paket geschehen soll, das auf die oben beschriebenen Parameter passt.

DROP verwirft das Paket. Das Paket führt niemals zu einem ISDN/PPP Verbindungsaufbau. Abhängig von den Debug-Einstellungen erscheint in der Logdatei ein Eintrag, dass dieses Paket verworfen wurde.

ACCEPT akzeptiert das Paket. Das Paket wird an die Gegenstelle weitergeleitet. Das Paket führt dabei evtl. zu einem ISDN/PPP Verbindungsaufbau.

RETURN beendet die Bearbeitung der Regeln dieser Tabelle und kehrt zur aufrufenden Tabelle zurück.

Tabellenname springt in der Bearbeitung zu der Chain mit dem Namen *Tabellenname* und vergleicht dort alle Regeln nacheinander mit dem IP Paket, bis eine Regel zutrifft. Die Verarbeitung kehrt zum Nachfolger der aktuellen Regel zurück, wenn in der Tabelle *Tabellenname* eine Regel zutrifft, die das Target RETURN enthält.

Beispiel: FWpartner

Standardeinstellung: Dieser Parameter ist zwingend erforderlich.

Description

Die Beschreibung der Regel ist optional und hat keine Auswirkung auf die Konfiguration von IP Tables. Die Beschreibung wird jedoch in der Konfigurationsdatei abgespeichert.

7.6 Format der Konfigurationsdatei

7.6.1 Abschnitt [IPTABLESSECTIONS]

Dieser Abschnitt enthält das Verzeichnis aller definierten Tabellen bzw. Regeln und deren Beschreibung.

IPTABLESSECT n = *Tabellenname*

Die Namen **IPTABLESECT** sind aufsteigend beginnend mit 0 numeriert. Bei der Speicherung der Konfiguration aus der Weboberfläche ergibt sich *Tabellenname* aus dem Bezeichner aus der Tabelle Firewall Sections. Jede Tabellenzeile ist in einem eigenen Abschnitt abgelegt, dessen Name sich aus dem Tabellennamen und einer fortlaufenden dreistelligen hexadezimalen Nummer zusammensetzt.

Beispiel: **IPTABLESSECT0** = **FWpartner**

Standardeinstellung: Dieser Parameter ist zwingend erforderlich.

IPTABLESDESC n = *Zeichenkette*

Optional kann zu jeder Tabelle eine textuelle Beschreibung vorliegen, welche die Aufgabe dieser Tabelle erläutert. Der Text kann sich über mehrere Zeilen erstrecken und sollte immer in Hochkommata eingeschlossen sein, da er typischerweise Leerzeichen enthält.

Beispiel: **IPTABLESDESC0** = "Zugang zur Datenbank der Partnerapotheke"

Standardeinstellung: leere Zeichenkette.

7.6.2 Abschnitt [*Tabellenname*_nnn]

Der Tabellenname wird von **IPTABLESECT n** referenziert und beschreibt eine Tabellenzeile aus der Weboberfläche. Die Tabellenzeilen sind über eine dreistellige hexadezimale Nummer beginnend von 001 aufsteigend durchnummeriert.

SrcIP = *IP-Nummer*

Beschreibung: IP-Nummer der Quelle. Dieser Wert ist in Punktschreibweise oder als DNS Name anzugeben. In Verbindung mit **SrcMask** beschreibt dieser Wert den IP-Nummernkreis des Ursprungs der Pakete, für welche diese Regel definiert ist.

Beispiel: **SrcIP** = 192.168.1.0

Standardeinstellung: 0.0.0.0

SrcMask = *Netzmaske*

Beschreibung: Netzmaske der Quelle. Dieser Wert ist in Punktschreibweise anzugeben.

Beispiel: **SrcMask** = 255.255.255.0

Standardeinstellung: 255.255.255.255

DstIP = *IP-Nummer*

Beschreibung: IP-Nummer des Ziels. Dieser Wert ist in Punktschreibweise oder als DNS Name anzugeben. In Verbindung mit **DstMask** beschreibt dieser Wert den IP-Nummernkreis des Ziels der Pakete, für welche diese Regel definiert ist.

Beispiel: **DstIP** = 192.168.129.0

Standardeinstellung: 0.0.0.0

DstMask = *Netzmaske*

Netzmaske des Ziels. Dieser Wert ist in Punktschreibweise anzugeben.

Beispiel: **DstMask** = 255.255.255.0

Standardeinstellung: 255.255.255.255

TCPPorts = *Portdefinition*

Die Portdefinition beschreibt einen oder mehrere TCP Ports, für welche diese Regel definiert ist. Die Schreibweise, wie mehrere Ports zu definieren sind, ist im Kapitel Portdefinitionen beschrieben. Das Schlüsselwort **any** bezeichnet beliebige TCP Ports. Das Schlüsselwort **all** bezeichnet alle TCP Ports.

Beispiel: **TCPPorts** = telnet

Standardeinstellung: any

UDPPorts = *Portdefinition*

Die Portdefinition beschreibt einen oder mehrere UDP Ports, für welche diese Regel definiert ist. Die Schreibweise, wie mehrere Ports zu definieren sind, ist im Kapitel Portdefinitionen beschrieben. Das Schlüsselwort **any** bezeichnet beliebige UDP Ports. Das Schlüsselwort **all** bezeichnet alle UDP Ports.

Beispiel: **UDPPorts** = netbios-ns

Standardeinstellung: any

Protos = Protokolldefinition

Die Protokolldefinition beschreibt ein oder mehrere Protokolle (TCP, UDP, ICMP, ESP, ...), für welche diese Regel definiert ist. Die Protokolldefinition **any** bezeichnet beliebige Protokolle.

Beispiel: **Protocols = ESP**

Standardeinstellung: **any**

Target = [DROP|ACCEPT|RETURN|Tabellenname]

Dieser Parameter bestimmt, was mit dem IP Paket geschehen soll, das auf die oben beschriebenen Parameter passt.

DROP verwirft das Paket. Das Paket führt niemals zu einem ISDN/DSL Verbindungsaufbau. Abhängig von den Debug Einstellungen erscheint in der Logdatei ein Eintrag, dass dieses Paket verworfen wurde.

ACCEPT akzeptiert das Paket. Das Paket wird an die Gegenstelle weitergeleitet. Das Paket führt dabei evtl. zu einem ISDN/DSL Verbindungsaufbau.

RETURN beendet die Bearbeitung der Regeln dieser Tabelle und kehrt zur aufrufenden Tabelle zurück.

Tabellenname springt in der Bearbeitung zu der Regel *Tabellenname_001* und vergleicht dort alle Regeln nacheinander mit dem IP Paket, bis eine Regel zutrifft. Die Verarbeitung kehrt zum Nachfolger der aktuellen Regel zurück, wenn in der Tabelle *Tabellenname* eine Regel zutrifft, die das Target RETURN enthält.

Beispiel: **Target = FWpartner**

Standardeinstellung: Dieser Parameter ist zwingend erforderlich.

Desc = Zeichenkette

Optional kann zu jeder Regel eine textuelle Beschreibung vorliegen, welche die Aufgabe dieser Regel erläutert. Der Text kann sich über mehrere Zeilen erstrecken und sollte immer in Hochkommata eingeschlossen sein, da er typischerweise Leerzeichen enthält.

Beispiel: **Desc = "Alle Netbios Pakete verwerfen"**

Standardeinstellung: *leere Zeichenkette*

7.7 Portdefinition

Mengen von Ports lassen sich auf bequeme Weise definieren, damit die Anzahl der Tabellenzeilen nicht überhand nimmt. Ein Bereich zusammenhängender Portnummern ist durch Angabe des ersten und letzten Ports getrennt durch Doppelpunkt (:) anzugeben. Eine Aufzählung von Portnummern ist durch Komma (,) zu trennen. Sowohl symbolische Portnamen entsprechend der Datei `/etc/services`, als auch Portnummern zwischen 1 und 65536 sind erlaubt. Der Wert `all` steht für alle Portnummern und ist somit eine Abkürzung für `1:65536`. Der Wert `any` bezeichnet beliebige Ports.

Hier folgt die formale Beschreibung von Portdefinition:

Portdefinition ::= all | any | Portliste

Portliste ::= Port | Port:Port | Portliste,Portliste

Port ::= Nummer | symbolischer Name

7.8 Protokolldefinition

Mengen von Protokollen lassen sich auf bequeme Weise definieren, damit die Anzahl der Tabellenzeilen nicht überhand nimmt. Eine Aufzählung von Protokollnummern ist durch Komma (,) zu trennen. Sowohl symbolische Protokollnamen entsprechend der Datei `/etc/protocols`, als auch Protokollnummern zwischen 1 und 255 sind erlaubt. Der Wert `any` bezeichnet beliebige Ports.

Hier folgt die formale Beschreibung von Portdefinition:

Protokolldefinition ::= any | Protokollliste

Protokollliste ::= Protokoll | Protokollliste,Protokollliste

Protokoll ::= Nummer | symbolischer Name

7.9 Tipps zur Konfiguration

Die letzte Regel einer benutzerdefinierten Chain, sollte auf alle Pakete passen und das Paket entweder verwerfen oder durchlassen, nicht jedoch ein RETURN ausführen, d. h.:

Beschreibung	Wert
Quell-IP-Adresse	0.0.0.0
Quell-IP-Maske	0.0.0.0
Ziel-IP-Adresse	0.0.0.0
Ziel-IP-Maske	0.0.0.0
TCP Ports	any
UDP Ports	any
Protokolle	any
Aktion	ACCEPT oder DROP

Tab. 2: Standardregel

Ohne diesen Eintrag kann es sein, dass ein Paket auf keine benutzerdefinierte Regel dieser Chain passt und die vordefinierte Regel am Ende der Chain auslöst, d.h. RETURN wird ausgeführt. Danach kommt das Paket in die isdn-d-fw Chain und läuft unter Umständen in eine weitere Chain, welche für eine andere Peer Station definiert ist. Dies kann gewollt sein, führt jedoch eher zu Verwirrung.

Die RETURN Aktion kann für eine Chain gewollt sein, wenn sie eine bestimmte Aufgabe erfüllen soll, die von mehreren anderen Chains benötigt wird, vergleichbar mit einem Unterprogramm. Eine solche Aufgabe ist z. B. das Verwerfen aller netbios Pakete.

7.10 Konfigurationsbeispiele

Beispiel 1: Zugang aller Rechner im LAN zum Internet mit Nameserver.

LAN: 210.21.1.0
Router Ethernet Schnittstelle: 210.21.1.106
Default Route auf allen Rechnern: 210.21.1.106.
Nameserver für alle Rechner: 210.21.1.106.

```
[PEERSECTIONS]
PEERSECT1 = arcor
```

```
[arcor]
PeerIP = 0.0.0.0
Netmask = 0.0.0.0
Call = 00192070
Listen = -
L2Prot = 5
NAT = 1
IP-Table = FWinternet
Timeout = 120
PPP = PPParcor
```

```
[IPTABLESSECTIONS]
IPTABLESSECT1 = FWinternet
IPTABLESDESC1 = "Alle Rechner aus dem LAN dürfen alles
ausser Netbios"
```

```
[FWinternet_001]
Target = DROP
SrcIP = 210.21.1.0
SrcMask = 255.255.255.0
DstIP = 0.0.0.0
DstMask = 0.0.0.0
TCPPorts = netbios-ns,netbios-dgm,netbios-ssn
UDPPorts = netbios-ns,netbios-dgm,netbios-ssn
Desc = "Keine Netbios Pakete erlauben"
```

```
[FWinternet_002]
Target = ACCEPT
SrcIP = 210.21.1.0
SrcMask = 255.255.255.0
DstIP = 0.0.0.0
DstMask = 0.0.0.0
Desc = "alle Rechner aus dem LAN dürfen raus"
```

```
[FWinternet_003]
Target = DROP
SrcIP = 0.0.0.0
SrcMask = 0.0.0.0
DstIP = 0.0.0.0
DstMask = 0.0.0.0
Desc = "Diese Regel bewirkt, dass kein RETURN ausgeführt
wird"
```

8 IPsec und VPN

Dieses Kapitel beschreibt die Funktionsweise der VPN Implementierung und die VPN Konfiguration in der Konfigurationsdatei `isdnd.cfg`. Die Konfiguration über die Weboberfläche geschieht entsprechend und sollte intuitiv verständlich sein.



Achtung: MULTIDATA empfiehlt aus Stabilitätsgründen und aus Kostengründen einen Internetzugangstarif zu verwenden, welcher es erlaubt, permanent Online sein zu können, wie z. B. eine Flatrate oder T-DSL Volumentarife. Damit der Router nach einer Zwangstrennung durch den ISP sofort wieder Online geht, muss der Konfigurationsparameter `idle` in den Menüs der Weboberfläche bzw. `Timeout` in der Konfigurationsdatei für die entsprechende Peer Station auf den Wert `-3` (Always-Online) gesetzt werden. Dann geht der Router automatisch beim Start bzw. nach einer Trennung wieder Online. Der Parameter `CallForOnline`, welcher in der Gegenstelle konfiguriert ist, kann dann leer bleiben.

Zur Konfiguration eines Heimarbeitsplatzes z. B. mit dem SafeNet Client gibt es ein gesondertes Dokument.

8.1 Anwendungsfälle

Einige Anwendungsfälle aus dem Apothekenumfeld:

- Fernwartung: Das Apothekensoftwarehaus wählt sich in das Apotheken LAN ein und greift dort auf verschiedene Rechner und Dienste transparent zu.
- Softwareupdate: Ein Rechner aus der Apotheke kontaktiert einen Updateserver.
- Partnerapotheke: Zwei oder mehr Apotheken tauschen Daten aus, z. B. für eine gemeinsame Warenwirtschaft.
- Heimarbeitsplatz: Ein einzelner Windows-PC ist direkt mit dem Internet über ein Modem, über eine ISDN Karte oder über DSL verbunden (Roadwarrior).
- Krankenhäuser (allgemein: Kunden) greifen auf die Apotheke zu
- Hub and Spoke: Mehrere Apotheken (Spoke) werden sternförmig über einen zentralen VPN Verteilerknoten (Hub) gekoppelt.

Bei allen Anwendungsfällen sollten die Netzwerkadressen der beteiligten privaten LANs konstant, eindeutig und aus einem privaten Nummernkreis (192.168.0.0 oder 10.0.0.0) sein. Es bietet sich an, jedem LAN ein Klasse-C-Netz zuzuweisen. Bei mehr als 250 LANs müssen Netzwerkadressen aus dem Nummernkreis der privaten Klasse-A-Netze 10.0.0.0 vergeben werden.



Die eindeutige Numerierung der Netzwerkadressen aller Apotheken sollte **Apothekensoftwarehaus übergreifend** geschehen.

Dies ist unerlässlich, wenn z. B. ein Krankenhaus mit mehreren Apotheken kommunizieren möchte, welche von unterschiedlichen Apothekensoftwarehäusern betreut werden. Die privaten Adressen aller beteiligten Apotheken müssen dann eindeutige private IP-Adressen haben. Im Nummernkreis 10.0.0.0 sind ca. 65000 Klasse-C-Netze verfügbar. Daher ist es möglich, jeder Apotheke ein eindeutiges Klasse-C-Netz zuzuweisen.

Falls dennoch private Netze mit identischer Netzwerkadressen verbunden werden müssen, gibt es die Möglichkeit, der Gegenstelle ein virtuelle private Adresse vorzuspiegeln. Dies geschieht mit Hilfe des Parameters `LocalVirtualNet` aus dem Kapitel 8.4.2 Abschnitt [VPNRouter].

8.2 DynDNS

HERMES-PRO unterstützt die Protokolle verschiedener DynDNS Server, bei denen er sich mit einem konfigurierbaren Namen registriert. Als IP-Adresse trägt er immer die Internetadresse ein, die er vom ISP zugeteilt bekommen hat.



Achtung: die Namensauflösung der IPSec Gegenstellen geschieht über den Nameserver des ISP und nicht über den konfigurierten DynDNS Server. Somit ist gewährleistet, dass unterschiedliche IPSec Gegenstellen auch unterschiedliche DynDNS Server verwenden können.

DynDNS Protokoll	Port	Optionen
GnuDIP	3495	
DynDNS	80	

Tab. 3: Unterstützte DynDNS Server

8.3 Interoperabilität

HERMES-PRO kann mit unterschiedlichen Gegenstellentypen VPN Tunnel aufbauen. Dabei müssen die Gegenstellen keine festen IP-Adressen haben und auch nicht permanent Online sein. Die Gegenstellen sollten sich jedoch zumindest an einem DynDNS Server anmelden.

8.3.1 Dynamische IP-Adressen

Eine besondere Fähigkeit von HERMES-PRO ist, dass er mit IPSec-Gegenstellen Verbindungen aufbauen kann, welche weder eine feste IP-Adresse haben, noch ständig online sind. Die IP-Adresse des entfernten Tunnelendpunktes ermittelt HERMES-PRO **dynamisch** und **fortlaufend** durch Nameserverabfragen. Die eigene IP-Adresse teilt er bei einer Internetverbindung einem DynDNS Server mit. Dies wird wiederholt, sobald der eigene Name nicht mehr korrekt aufgelöst werden kann.

Die Gegenstelle kann mittels ISDN Anruf dazu veranlasst werden, Online zu gehen. HERMES-PRO geht selber Online, wenn er dazu aufgefordert wird. Das Kapitel Callback beschreibt die unterstützten Callback Mechanismen. CLIP Callback ist anderen Verfahren vorzuziehen, da keine Telefongebühren anfallen. Dabei kann die Konfiguration jedoch umfangreich werden, wenn man sich von von mehreren Gegenstellen aufwecken lassen will.

HERMES-PRO kann mit beliebigen VPN Routern Verbindungen aufbauen, welche immer online sind und eine feste IP-Adresse haben. Wenn die Gegenstelle keine feste IP-Adresse hat, dann muß sie ihre IP-Adresse einem beliebigen DynDNS Server mitteilen. Wenn die Gegenstelle nicht immer online ist, dann muss sie ein kompatibles Callbackverfahren unterstützen. Wenn die Gegenstelle zwar DynDNS jedoch kein Callback unterstützt, dann kann der Verbindungsaufbau nur in eine Richtung erfolgen, wie z. B. bei einem Windows-PC (Roadwarrior).

8.3.2 Parameteraushandlung mit ISAKMP

Das Protokoll ISAKMP (Internet Security Association and Key Management Protocol) dient dazu, verschiedene Sicherheitsparameter auszuhandeln. Unter anderem wird dabei Schlüsselmaterial ausgetauscht: IKE (Internet Key Exchange).

Das Protokoll läuft in zwei Phasen ab. In beiden Phasen werden Parameter ausgehandelt. Die Aushandlung ist erfolgreich, wenn beide Seiten alle Parameter der Gegenseite akzeptieren.

In der **Phase 1** des ISAKMP kommt der Main Mode (Identity Protection) oder der Aggressive Mode zum Einsatz. Als Authentifizierungsmethode dient ein konfigurierbarer, vorinstallierter Schlüssel (Preshared Key).

Parameter	Senden	Akzeptieren
Verschlüsselung	3DES-CBC	3DES-CBC
Hashverfahren	SHA	SHA
Authentifizierung	Preshared Key	Preshared Key
Diffie Hellmann Gruppe	1024 Bit MODP (2)	alle
Lebensdauer	3600 Sekunden	60 Sek bis 8 Stunden. Keine Kilobytes
Identifikation	eigener FQDN	entfernter FQDN ¹

Tab. 4: Phase 1 Parameter

Für jede VPN-Route (s. u.) wird bei Bedarf eine eigenständige **Phase 2** (Quick Mode) durchgeführt, welche eine Security Association (SA) erzeugt.

Parameter	Senden	Akzeptieren
Verschlüsselung	3DES-CBC	3DES-CBC
Authentifizierung	HMAC-MD5	HMAC-MD5
Lebensdauer	1200 Sekunden	alle
Kapselung	Tunnel	Tunnel
PFS Gruppe	keine	alle
eigene Identifikation ²	Ethernet IP/Maske	Ethernet IP/Maske
entfernte Identifikation	VPN-Route	alle

Tab. 5: Phase 2 Parameter

ISAKMP benötigt die IP-Adresse des entfernten Tunnelendpunkts, damit die richtigen Konfigurationseinstellungen verwendet werden können. Alternativ kann bei eingehenden Verbindungen der Aggressive Mode zum Einsatz kommen, bei dem die Gegenstelle anhand der Identifikation der Phase 1 erkannt wird.

¹ Wenn die IP-Adresse der Gegenstelle bekannt ist, dann wird alles akzeptiert.

² In der Phase 2 schickt der Initiator zwei Identifikationen, welche als Routinginformationen für den Empfänger dienen können. Dabei sind IP-Adressen oder IP-Subnetze möglich.

8.3.3 Manuelle Schlüsselkonfiguration

Statt ISAKMP kann die manuelle Schlüsselkonfiguration eingesetzt werden. Dazu muss das Schlüsselmaterial (SharedSecret) und der Parameter SPI manuell eingegeben werden. Die Datenübertragung kann beginnen, sobald die IP-Adressen der Tunnelendpunkte bekannt sind.

Beim der manuellen Schlüsselkonfiguration unterstützt HERMES-PRO das symmetrische Verschlüsselungsverfahren 3DES mit 192 Bit Verschlüsselung.

Verfahren	Algorithmus
Verschlüsselung	3DES-CBC
Authentifizierung	keine

Tab. 6: Manuelle Konfiguration

8.3.4 Dead Peer Detection (DPD)

Routerimages ab V3.14 unterstützen DPD für **IKE** Gegenstellen. Wenn bei der Phase 1 Aushandlung festgestellt wird, dass die Gegenstelle DPD unterstützt, dann sendet der HERMES-PRO alle 12 Sekunden ein R_U_THERE Paket an die Gegenstelle. Wenn die Gegenstelle dies nicht beantwortet, dann versucht HERMES-PRO 5 mal im Abstand von jeweils 5 Sekunden die Gegenstelle zu erreichen. Also wird spätestens nach 37 Sekunden erkannt, dass die Gegenstelle nicht mehr erreichbar ist. In diesem Fall baut HERMES-PRO die IPSec Verbindung ab.

8.3.5 NAT-Traversal

Routerimages ab V3.23 unterstützen NAT-Traversal nach RFC 3947 und ebenfalls die Kompatibilitätsmodi draft-ietf-ipsec-nat-t-ike-02 und draft-ietf-ipsec-nat-t-ike-03. NAT-Traversal wird benötigt, wenn zwischen den IPSec Gegenstellen eine Network Address Translation (NAT) durchgeführt wird. Dies ist z. B. beim Anwendungsfall Heimarbeitsplatz gegeben, wenn gleichzeitig von mehreren Windows PCs hinter einem Einwahlrouter auf eine Apotheke zugegriffen werden soll.

Bei NAT-Traversal werden die IKE Pakete an den UDP Port 4500 (statt 500) gesendet. Die ESP Pakete werden in UDP verpackt, welche ebenfalls zum Port 4500 gesendet.

8.4 Format der Konfigurationsdatei

8.4.1 Abschnitt [IPSecn]

Die Abschnitte sind aufsteigend beginnend mit 1 nummeriert. Jeder Abschnitt definiert die Parameter für einen entfernten Tunnelendpunkt, mit welchem der lokale Router über einen gesicherten Tunnel IP Pakete austauschen kann. Welche Pakete durch welchen Tunnel geleitet werden, bestimmt der Abschnitt [VPNRouter] (siehe unten).

PeerName = Voll qualifizierter Internet Domänen Name

Der Name des entfernten Tunnelendpunkts als FQDN (Full Qualified Domain Name). Der entfernte Tunnelendpunkt wird in der Literatur auch als VPN Gateway oder Remote VPN Gateway bezeichnet. Die VPN Software versucht diesen Namen fortwährend in eine IP-Adresse aufzulösen, solange eine Internetverbindung besteht und erkennt dadurch, ob die Gegenstelle online oder offline ist.

Achtung: die Namensauflösung der IPSec Gegenstellen geschieht über den Nameserver des ISP und nicht direkt über den konfigurierten DynDNS Server. Somit ist gewährleistet, dass unterschiedliche IPSec Gegenstellen auch unterschiedliche DynDNS Server verwenden können.

Sobald die Gegenstelle online geht, wird erwartet, dass sie sich mit **PeerName** bei einem DynDNS Server anmeldet. Die lokale VPN Software richtet dann einen VPN Tunnel ein.

Sobald die Gegenstelle offline geht, wird erwartet, dass sie sich beim DynDNS Server abmeldet. Dies kann entweder durch das Löschen des DNS Eintrags geschehen oder durch die Zuweisung der IP-Adresse 0.0.0.0 zu **PeerName**. Die VPN Software löscht dann den Tunnel.

Wenn die Gegenstelle eine feste IP-Adresse hat und immer im Internet verfügbar ist, dann existiert der VPN Tunnel solange HERMES-PRO eine Internetverbindung hat. Der Parameter **PeerName** kann in diesem Fall eine IP-Adresse in Punktnotation enthalten.

Beispiel: **PeerName = apo1.dyn.multidata.de**

Standardeinstellung: Dieser Parameter ist zwingend erforderlich.

KeyingMode = Manual oder **IKE**

Manuelle Parameterkonfiguration oder automatische Parameteraus-handlung durch IKE mittels des ISAKMP Protokolls.

Beispiel: **KeyingMode = Manual**

Standardeinstellung: Dieser Parameter ist zwingend erforderlich.

SPI = (Hexadezimal)Zahl

Relevant für: **KeyingMode = Manual**

Security Parameter Index. Der SPI ist 32 Bit groß und in jedem verschlüsselten bzw. authentifizierten Paket enthalten, um IPsec eine Zuordnung zu den Sicherheitsparametern zu ermöglichen. HERMES-PRO verwendet den gleichen SPI sowohl für abgehende als auch für eingehende Pakete. Der SPI muss für beide Tunnelendpunkte gleich sein.

Wenn IKE zum Einsatz kommt, dann erzeugt der Keying Daemon automatisch SPIs.

Der SPI muss größer oder gleich 0x200 sein.

Beispiel: **SPI = 0x210**

Standardeinstellung: **0xFFFFFFFF**

SharedSecret = Zahlenschlüssel

Relevant für: **KeyingMode = Manual**

Schlüssel zur symmetrischen Datenverschlüsselung mittels 3DES. Das Format des 192 Bit langen Schlüssels ist eine Hexadezimalzahl, die aus sechs Achtergruppen besteht, welche mit "_" unterteilt sind.

Wenn IKE zum Einsatz kommt, dann erzeugt es automatisch SharedSecrets

Beispiel:

sharedSecret = 0x12345678_22345678_32345678_42345678_52345678_62345678

Standardeinstellung: Dieser Parameter ist für **KeyingMode = Manual** zwingend erforderlich

PresharedKey = Kennwort

Relevant für: **KeyingMode = IKE**

Die IKE Aushandlung verwendet dieses Kennwort zur Authentifizierung der Gegenstelle. Die Gegenstelle muss für einen erfolgreiche Authentifizierung das gleiche Kennwort verwenden.

Die Wahl des Kennworts sollte den üblichen Richtlinien für Kennwörter entsprechen.

Beispiel: **PresharedKey = geh_Heim_nis**

Standardeinstellung: Dieser Parameter ist für **KeyingMode = IKE** zwingend erforderlich

Phase1Mode = Main oder **Aggressive**

Relevant für: **KeyingMode = IKE**

Die IKE Aushandlung verwendet diesen Modus in der Phase 1 Aushandlung. Der Aggressive Modus wird für Gegenstellen benötigt, welche mit dynamischen IP-Adressen in Verbindung mit dem Main Modus nicht zurecht kommen (z. B. BinTec Router, Sonicwall Router mit Konfiguration der Phase 1 Identifikation vom Typ FQDN). Die IPSec Implementierung von Microsoft unterstützt keinen Aggressive Modus.

Der Aggressive Modus benötigt weniger Nachrichten zur Aushandlung, aber er gilt als unsicherer als der Main Modus.

Beispiel: **Phase1Mode = Aggressive**

Standardeinstellung: **Main**

AutoTunnelUp = Yes oder **No**

Relevant für: **KeyingMode = IKE**

Auto Tunnel Up (ATU) steuert das Verhalten des IKE-Verbindungsaufbaus. Wenn **AutoTunnelUp** den Wert **Yes** hat, dann baut HERMES-PRO die IKE Verbindung zur Gegenstelle auf, sobald **PeerName** in eine IP-Adresse aufgelöst werden kann, d. h. sobald die Gegenstelle online ist.

Ansonsten baut HERMES-PRO die IKE Verbindung erst dann auf, wenn Daten zu übertragen sind.

Beispiel: **AutoTunnelUp = Yes**

Standardeinstellung: **No**

RouteToTunnelEndpoint = direct oder **"via VPN"**

Relevant für: **KeyingMode = IKE**

Dieser Parameter steuert, ob eine automatische VPN Route für die IP-Adresse des entfernten Tunnelendpunkts erstellt werden soll. Diese VPN Route wird benötigt, wenn die private IP-Adresse der Gegenstelle mit der IP-Adresse des Tunnelendpunktes identisch ist. Dies ist z. B. bei einem Softwareclient ohne virtuelle IP-Adresse der Fall.

Beispiel: **RouteToTunnelEndpoint = "via VPN"**

Standardeinstellung: **"direct"**

CallForOnline = Peer Abschnittsname

Relevant für: **KeyingMode = Manual** und **IKE**

Wenn die Gegenstelle nicht Online ist, fordert der Router die Gegenstelle dazu auf, Online zu gehen. Dazu ruft der Router die konfigurierte Gegenstelle über ISDN an. Es wird erwartet, dass die Gegenstelle so konfiguriert ist, dass sie mittels Callback Mechanismus eine Verbindung zum ISP aufbaut und somit Online geht.

Alle implementierten Callbackverfahren sind anwendbar. Siehe auch Kapitel Callback.

Wenn die Gegenstelle "Always Online" ist, kann dieser Parameter leer bleiben. Dann startet der Router kein ISDN Anruf.

Standardeinstellung: leer

8.4.2 Abschnitt [VPNRouter]

Dieser Abschnitt enthält Routing-Informationen für virtuelle private Netze. Bei einfachen Konfigurationen wird es für jeden [IPSecn] Abschnitt genau einen [VPNRouter] Abschnitt geben.

Wenn über einen entfernten Tunnelendpunkt mehrere virtuelle private Netze erreichbar sind, dann müssen Sie hier mehrere Abschnitte anlegen, welche auf den gleichen Tunnelendpunkt verweisen (Hub and Spoke Architektur).



Wenn der entfernte Tunnelendpunkt ein Softwareclient ohne virtuelle IP-Adresse ist, dann muss keine Route angegeben werden. Die IP-Adresse des entfernten Tunnelendpunktes wird im IKE Modus automatisch der Routingtabelle hinzugefügt, wenn der Parameter **RouteToTunnelEndpoint = "via VPN"** aus dem [IPSecn] Abschnitt konfiguriert ist.

Die Abschnitte sind aufsteigend, beginnend mit 1 numeriert.

PeerIP = IP-Adresse

IP-Netzwerkadresse des entfernten Netzwerks in Punktnotation. Diese IP-Adresse wird sowohl in der IP-Routing Tabelle als auch in der VPN-Routing Tabelle aufgenommen. **PeerLANIP** muss für alle **IPSecn** Abschnitte eindeutig sein.

Beispiel: **PeerLANIP = 192.168.10.0**

Standardeinstellung: Dieser Parameter ist zwingend erforderlich.

Netmask = Netzwerkmaste

Netzwerkmaste des entfernten Netzwerks in Punktnotation.

Beispiel: **PeerLANMask** = 255.255.255.0

Standardeinstellung: 255.255.255.0

PeerTunnelEndpoint = *PeerName* aus [IPSecn]

Entfernter Tunnelendpunkt, zu welchem der Routingprozess die Pakete leiten soll. Es muss ein Abschnitt [IPSecn] geben, in welchem der Wert **PeerName** mit dem hier angegebenen Namen übereinstimmt.

Falls der Wert leer ist oder auf keinen [IPSecn] Abschnitt verweist, dann hat der gesamte [VPN Routen] Abschnitt keine Auswirkungen.

Beispiel: **PeerTunnelEndpoint** = apo2.dyn.multidata.de

Standardeinstellung: leer

LocalVirtualNet = *IP-Netzwerkadresse*

IP-Netzwerkadresse unter welcher das lokale Netz aus dem entfernten Netz erreichbar ist (lokale virtuelle Netzwerkadresse).

Dieser Parameter wird z. B. für die Erreichbarkeit von LANs benötigt, welche die selbe Netzwerkadresse (z. B. 192.168.1.0) haben. Der Parameter wird dazu verwendet, eine Netzwerkadressumsetzung der lokalen IP-Adressen vorzunehmen. Das lokale Netzwerk scheint für die Gegenstelle die (eindeutige) Netzwerkadresse **LocalVirtualNet** zu haben.

Die Netzwerkadresse muss zur eingestellten Netzwerkmaske der Ethernetschnittstelle passen, d. h. alle Bits, welche in der Netzwerkmaske der Ethernetschnittstelle 0 sind müssen auch in **LocalVirtualNet** 0 sein. Wenn der Parameter leer ist, dann wird keine Netzwerkadressumsetzung durchgeführt.

Das Routing bzw. die Phase 2 der Gegenstelle muss mit **LocalVirtualNet** konfiguriert werden.

Beispiel: **LocalVirtualNet** = 10.10.10.0

Standardeinstellung: leer (keine Netzwerkadressumsetzung)

8.4.3 Abschnitt [DynDNS]

Dieser Abschnitt wird nur benötigt, wenn HERMES-PRO bei einer Interneteinwahl die IP-Adresse automatisch einem DNS Server mitteilen soll. Unterschiedliche DynDNS Server benötigen unterschiedliche Parameter (siehe Tabelle in Kapitel DynDNS). Eine Konfigurationsänderung der folgenden Parameter wird aktiv, sobald die Konfiguration gespeichert wird ([Save configuration to files](#)) und die nächste Interneteinwahl geschieht.

Hostname = Voll qualifizierter Internet Domänen Name

Diese Name wird dem DynDNS Server mitgeteilt.

Beispiel: **Hostname = ap01.dyn.multidata.de**

Standardeinstellung: Dieser Parameter ist zwingend erforderlich.

Protocol = DynDNS Protokoll

Dieses Protokoll wird zur Bekanntgabe der IP-Adresse verwendet. Die unterstützten Protokolle sind in *Tab. 3: Unterstützte DynDNS Server* aufgeführt.

Beispiel: **Protocol = gnudip**

Standardeinstellung: **gnudip**

User = Zeichenkette

Dieser Parameter wird dem DynDNS Server als Benutzername mitgeteilt.

Beispiel: **User = ap01**

Standardeinstellung: Dieser Parameter ist zwingend erforderlich.

Password = Zeichenkette

Dieser Parameter wird dem DynDNS Server als Kennwort mitgeteilt.

Beispiel: **Password = dyndnspasswd**

Standardeinstellung: Dieser Parameter ist zwingend erforderlich.

Server = IP-Adresse

Die IP-Adresse oder FQDN des DynDNS Servers. Soll eine von Standard abweichende Portnummer verwendet werden, dann kann die Adresse in der Form *Server:Port* angegeben werden.

Beispiel: **Server = ns.multidata.de**

Standardeinstellung: Dieser Parameter ist zwingend erforderlich.

8.5 Firewall-Einstellungen

Die Firewall ist so eingestellt, dass nur Pakete an den Port 500 (isakmp) den Port 4500 (NAT-T) und Pakete des ESP und des ICMP Protokolls den Router erreichen. Diese Regeln werden automatisch aktiv, sobald eine Internetverbindung besteht. TCP und UDP Verbindungen vom LAN in das Internet sind nicht betroffen. Das Verhalten des Routers ändert sich im Vergleich zur Version ohne IPSec nicht.

Destination IP-Address	UDP Ports	Protocols	Target
<i>Dynamische IP Adresse</i>	500	esp,icmp	ACCEPT
<i>Dynamische IP Adresse</i>	Any	Any	REJECT

Tab. 7: automatische Firewall-Regeln

Der Verkehr zwischen privaten LANs und die Einschränkung des Internetzugangs für LAN Computer lässt sich über die üblichen Methoden konfigurieren.

9 CAPI-Serverfunktion

9.1 Grundlagen

CAPI Applikationen von einem oder mehreren Windows PCs (Clients) können mit Hilfe der VCAPI die ISDN-Hardware des Routers HERMES-PRO/X (Server) nutzen. Den CAPI-Applikationen wird eine capi2032.dll und eine capi20.dll als Schnittstelle zur Verfügung gestellt. Es wird keine Schnittstelle auf Device Driver Level zur Verfügung gestellt (siehe *capi 1999*, Teil 2). NDIS-Wrapper oder Anwendungen wie z.B. CFOS, die auf diesen Schnittstellen aufsetzen, können die VCAPI nicht nutzen. Die capi2032.dll auf dem Client kommuniziert über die Socket-Schnittstelle mit dem Server-Prozeß.

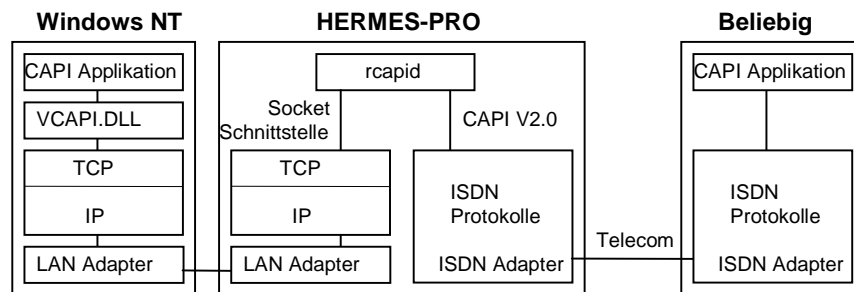


Abb. 9.1: VCAPI Übersicht

9.2 Client

Als Client Betriebssystem kann Windows NT und Windows 95 zum Einsatz kommen. Jede CAPI Applikation, die auf capi2032.dll oder capi20.dll aufsetzt, sollte lauffähig sein.

Bisher wurden folgende Applikationen unter Windows NT 4.0 getestet:

- testhsc (MULTIDATA)
- T-Online

- RVS-COM (V1.701)
- WinFax Pro 9.0

9.2.1 Konfiguration von capi2032.dll

Die Datei *capi2032.dll* (im Bild mit *VCAPL.DLL* bezeichnet) muß sich im Verzeichnis *%SystemRoot%\system32* befinden, um von allen Anwendungen gefunden zu werden.

Die IP Adresse und die Portnummer des VCAPL Servers (*rcapid*) muß in der Registry mit dem Programm *regedit.exe* eingetragen werden:

- *HKEY_LOCAL_MACHINE\SOFTWARE\MULTIDATA\VCAPL\Client*
- *VCAPL_SERVER_ADDR*
die IP Nummer des Servers in Punktschreibweise als Zeichenkette.
- *VCAPL_SERVER_PORT_NO*
die Portnummer des VCAPL Service (7703) als Zeichenkette.

Die symbolischen Rechnernamen des Clients und des Servers sollten in der Datei

%SystemRoot%\system32\drivers\etc\hosts

und der Dienst mit dem Namen *vcapi* sollte in der Datei

%SystemRoot%\system32\drivers\etc\services

eingetragen werden, damit keine unnötigen Wartezeiten bei Statusabfragen, z.B. mit dem *netstat* Kommando auftreten.

9.2.2 16-Bit Anwendungen

Es gibt noch einige 16-Bit Anwendungen, die auf der *capi20.dll* aufsetzen. Die verwendete *capi20.dll* muß sich in dem Verzeichnis *%SystemRoot%\system* befinden, um von allen Anwendungen gefunden zu werden. Die *capi20.dll* enthält nur eine Umsetzung auf die *capi2032.dll* und muß deshalb nicht konfiguriert werden.

9.3 Server

Der Serverprozeß heißt *rcapid*. Der Prozeß wird zur Boot-Zeit automatisch gestartet und muß nicht konfiguriert werden.

Der Hintergrundprozeß *rcapid* nimmt standardmäßig Verbindungen mit dem TCP-Service *vcapi* auf Port 7703 auf allen Netzwerkschnittstellen entgegen.

10 Konfiguration

Die Konfiguration von HERMES-PRO/X kann über einen Web-Browser und über die Konfigurationsdateien

- /usr/lib/hermes/isdnd.cfg
- /etc/ihosts
- /etc/hosts

erfolgen. Für fast alle Konfigurationsparameter gibt es Standard-einstellungen, die verwendet werden, wenn der Parameter nicht angegeben wird.

Alle Einstellungen über den Web-Browser werden sofort wirksam, falls dies nicht anders angegeben ist. Die Konfigurationsdateien werden nicht automatisch aktualisiert. Der Menüpunkt *Save configuration to files* speichert eine mit dem Web-Browser eingestellte Konfiguration in den Konfigurationsdateien ab. Geänderte Konfigurationsdateien, wie sie z.B. mittels *ftp* auf den Router übertragen werden können, werden mit der Auswahl des Menüpunkts *Read configuration from files* aktiv. Wahlweise kann mit dem *kill* Kommando dem *isdnd* Prozeß das Signal 1 geschickt werden. Damit eine Konfiguration nach dem Neustart des Routers wieder zur Verfügung steht, müssen die Konfigurationsdateien zuerst mit dem Menüpunkt *Save configuration to files* abgespeichert und dann mit dem Menüpunkt *Write files to Flash ROM* persistent abgelegt werden.

10.1 Konfiguration über einen Web-Browser

Im folgenden werden die verschiedenen Menüs beschrieben, die eine Konfiguration über einen beliebigen Web-Browser ermöglichen. Die Konfigurationsmenüs sind über folgende Adresse erreichbar:

<http://IP-Adresse:7705/>

10.1.1 General Router

Dieses Menü erlaubt allgemeine Einstellungen, die die Routingsoftware und die Konfiguration über einen Web-Browser betreffen.

MSN	MSN Wakeup Signal	Port	Timeout	Journaling Port	Debug	Timeserver	
8	9	7705	30	514	0123456	210.21.1.12	edit

MSN = *Mehrfachrufnummer*

Die MSN (Multiple Subscriber Number, Mehrfachrufnummer), die das ISDN Gerät von anderen ebenfalls angeschlossenen Geräten oder Softwareprogrammen unterscheidet. Die letzten Ziffern der Nummer, welche durch Ihre Nebenstellenanlage/Vermittlungsstelle als Rufnummer des Angerufenen (Called Party Number) signalisiert wird, wird mit der angegebenen MSN verglichen. Bei Gleichheit wird der Ruf angenommen, sonst wird er ignoriert, damit ein anderes Endgerät die Möglichkeit hat, den Ruf anzunehmen. Ist die Nummer nicht angegeben (leeres Eingabefeld), dann wird der MSN Vergleich nicht durchgeführt und der Ruf immer angenommen. Bei abgehenden Rufen teilt HERMES die MSN der Nebenstellenanlage/Vermittlungsstelle als eigene Nummer mit (Calling Party Number).

Die Standardeinstellung beträgt 1

MSN Wakeup Signal = *Mehrfachrufnummer*

Mehrfachrufnummer gibt die MSN an, die bei ankommenden Rufen mit der Rufnummer des Angerufenen (Called Party Number) verglichen wird. Wenn die letzten Ziffern übereinstimmen, wird das Signal RI der V.24-Schnittstelle für 100ms aktiviert. Hiermit kann z. B. eine USV bzw. ein Server ferngesteuert eingeschaltet werden. Auf die Rufannahme hat diese Funktionalität keine Auswirkung. Insbesondere kann `MSNWakeupSignal` gleich `MSN` sein. Mit `unset` kann diese Funktion deaktiviert werden. Bei leerer Eingabe wird bei jedem ankommenden Ruf das Signal RI aktiviert.

Die Standardeinstellung ist `unset`.

Port = *TCP Portnummer*

Die Nummer, unter der die HTTP-Schnittstelle zur Konfiguration (Web-Browser-Schnittstelle) erreichbar ist. Der Standardwert ist 7705. Dies ist eine freie Portnummer, die von beliebigen Programmen benutzt werden darf. HTTP-Server verwenden normalerweise den zugewiesenen Port

80; damit keine Konflikte zwischen den Programmen entstehen, wurde der freie Port 7705 verwendet. Die Änderung der Portnummer wird erst nach Neustart wirksam.

Die Standardeinstellung beträgt 7705

Timeout = Sekunden

Gibt die Haltezeit für die Verbindung in Sekunden an, siehe Kapitel 6.5, Verbindungsabbau.

Die Standardeinstellung beträgt 30

Journaling Port = UDP Portnummer

Das Journaling wird über diese Konfigurationsoption aktiviert. Wenn der Eintrag fehlt oder leer ist, erzeugt isdnd keine Journaling Nachrichten. Die Portnummer für das syslog Protokoll ist 514. Die empfohlene Portnummer für eine proprietäre MULTIDATA Client/Server Kommunikation ist 7707. Weitere Hinweise zum Journaling finden sie im Journaling Handbuch.

Standardeinstellung ist leer

Debug = Zeichenkette

Gibt an, welche Logausgaben in die Datei `/usr/lib/hermes/isdnd.log` erfolgen sollen. In Anhang B.5 sind die möglichen Einstellungen näher erläutert.

Die Standardeinstellung ist 012346

Timeserver = IP-Nummer

IP-Nummer oder symbolischer Name des Timeservers, von welchem der Router beim Start das aktuelle Datum und die Uhrzeit erfragt und als Systemzeit setzt. Ist dieses Feld leer, wird keine Einstellung des Datums und der Uhrzeit vorgenommen. Änderungen werden erst bei Neustart des Routers aktiv.

Die Standardeinstellung ist leer

10.1.2 Accounting Restricted Dialout

Zur Vermeidung von unerwünschten Verbindungsentgelten bei Fehlkonfiguration der Routingsoftware oder von CAPI-Anwendungen bietet HERMES-PRO/X die Option *Accounting Restricted Dialout* (ARD) an. Dabei werden in einem bestimmten Zeitintervall Informationen über

1. die Summe der signalisierten Gebühreneinheiten
2. die Anzahl der abgehenden Verbindungen
3. die Summe der Verbindungszeiten für abgehende Verbindungen

gesammelt. Sobald einer der drei Grenzwerte erreicht ist, wird von HERMES-PRO/X keine abgehende Verbindung mehr aufgebaut. In der Logdatei wird ein entsprechender Eintrag vorgenommen. Eingehende Rufe werden nach wie vor angenommen.

Die gesammelten Informationen können manuell zurückgesetzt werden.

Die Grenzwerte zu 2. und 3. wurden für den Fall eingeführt, daß die Summe der signalisierten Gebühreneinheiten nicht den tatsächlichen Gebühren entspricht. Es werden z.B. keine Gebühreneinheiten signalisiert, wenn das Dienstmerkmal nicht beantragt wurde oder ein abgehender Ruf über einen Call-by-Call-Provider vorgenommen wird.

Bereits aufgebaute Verbindungen werden nur über den normalen Verbindungs-Timeout ausgelöst. ARD bietet keine Möglichkeit eine Verbindung nach einer gewissen Zeit zu trennen. Die Option *Inaktivitätstimer* der ISDN-Protokollsoftware kann dazu genutzt werden, bei Fehlverhalten von Anwendungen unerwünschte Gebühren zu vermeiden. Diese Option überwacht nicht nur das TCP/IP-Routing, sondern beliebige ISDN-Anwendungen (z.B. alle VCAPI-Anwendungen). Wenn in einer konfigurierbaren Zeitspanne keine Nutzdaten mit der Anwendung ausgetauscht werden, wird die entsprechende Verbindung getrennt.

Die Einstellung des Inaktivitätstimers wird in Kapitel **Fehler! Verweisquelle konnte nicht gefunden werden.**, **Fehler! Verweisquelle konnte nicht gefunden werden.**, beschrieben.

Interval	Count	Charges	Duration	
-1	-1	-1	-1	edit

Interval = Stunden

Gibt die Größe des überwachten Zeitintervalls in Einheiten von Stunden an. Der Wert -1 schaltet die Überprüfung aller Grenzwerte aus.

Die Standardeinstellung beträgt -1.

Count = Anzahl

Gibt die Anzahl der abgehenden Verbindungen an. Der Wert -1 schaltet die Überprüfung dieses Grenzwertes aus.

Die Standardeinstellung beträgt -1.

Charges = Gebühreneinheiten

Gibt die Summe der signalisierten Gebühreneinheiten an. Falls Gebühren in nationaler Währung signalisiert werden, werden diese z.Zt. ignoriert. Der Wert -1 schaltet die Überprüfung dieses Grenzwertes aus.

Die Standardeinstellung beträgt -1.

Duration = Minuten

Gibt die Summe der Verbindungszeiten für abgehende Verbindungen in Minuten an. Der Wert -1 schaltet die Überprüfung dieses Grenzwertes aus.

Die Standardeinstellung beträgt -1.

10.1.3 Hosts Database

Dieses Menü erlaubt die Zuordnung von symbolischen Hostnamen zu IP-Nummern. Die Angaben werden in der Datei `/etc/hosts` verwaltet. Die Namen dienen dazu, eine Konfiguration übersichtlicher zu gestalten. Jeder Konfigurationsparameter, der eine IP-Nummer enthält, kann ebenso mit dem entsprechenden symbolischen Hostnamen spezifiziert werden.

Ein Nameserver-Dienst ist in der vorliegenden Version von HERMES-PRO/X nicht vorgesehen.

IP Number	Hostname and Aliases		
127.0.0.1	localhost	edit	delete
210.21.1.1	multi1	edit	delete
210.21.1.2	multi2	edit	delete
210.21.1.3	multi3	edit	delete

IP-Number

Geben Sie hier die IP-Nummer in Punktschreibweise an.

Hostname and Aliases

Geben Sie hier zuerst den offiziellen Namen des Hosts an, danach können Sie noch -getrennt mit Leerzeichen- weitere Aliasnamen vergeben.

Ein optionaler Kommentar beginnt mit dem # -Zeichen.

10.1.4 IP Interfaces

Dieses Menü erlaubt die Zuordnung von IP-Nummern und -Masken zu IP-Schnittstellen. Beachten Sie für die Ethernet-Schnittstellen auch das Kapitel 6, Ethernet-Switch.

Section Name	Ethernet	Ethernet IP	Ethernet Mask	ISDN Interface	ISDN Router	
INTERFACES	10 MBit	192.168.1.1	255.255.255.0	192.168.3.1	192.168.4.1	edit

Ethernet

Die Übertragungsgeschwindigkeit der Ethernetschnittstelle: 10 Mbit oder 100 MBit

Die Standardeinstellung beträgt 10 MBit

Ethernet IP

Die IP Nummer der Ethernetschnittstelle.

Die Standardeinstellung beträgt 192.168.1.1

Ethernet Mask

Die Netzmaske für die Ethernetschnittstelle.

Die Standardeinstellung beträgt 255.255.255.0

ISDN Interface

Dies ist die IP Nummer, unter der die IP Schicht von HERMES-PRO/X über ISDN erreichbar ist.

Die Standardeinstellung beträgt 192.168.3.1

ISDN Router

Dies ist die IP Nummer, unter der der isdnd Prozeß erreichbar ist. Diese IP Nummer ist zur Zeit nicht von Bedeutung.

Die Standardeinstellung beträgt 192.168.4.1

10.1.5 DHCP Server

Dieses Menü zeigt die Liste der DHCP Clients an. Die Untermenüs *Activation and Range* und *Fixed Mapping of MAC Addresses* dienen der Konfiguration.

Der DHCP Server weist Clients eine IP-Adresse aus einem konfigurierbaren Bereich zu. Zusätzlich kann eine direkte Zuordnung der MAC Adresse zu einer IP-Adresse vorgenommen werden. Die IP-Adressen müssen in dem Bereich des lokalen Netzwerks liegen (siehe Ethernet Adresse im Abschnitt IP Interfaces). Zusätzlich teilt der DHCP Server den Clients folgende Informationen mit:

- Subnet Mask: die Netzmaske des lokalen Netzwerks
- Router: die LAN IP-Adresse des HERMES Routers
- Domain Name Server: die LAN IP-Adresse des HERMES Routers
- Lease Time: Ein Tag

Activation and Range

Active	Start Address	End Address	
Yes	192.168.1.128	192.168.1.192	edit

Active = Yes | No

Dieser Parameter aktiviert den DHCP Server, wenn der Wert auf **Yes** steht. Beim Wert **No** ist der DHCP Server deaktiv. Eine Änderung hat sofortige Auswirkung.

Die Standardeinstellung beträgt **No**

Start Address = IP-Adresse

Dies ist die erste Adresse eines Adressbereichs, aus welchem der DHCP Server Adressen vergibt. Die IP-Adresse muss in dem Bereich des lokalen Netzwerks liegen (siehe Abschnitt IP Interfaces).

Dieser Parameter ist zwingend erforderlich, wenn Active auf **Yes** steht.

End Address = IP-Adresse

Dies ist die letzte Adresse eines Adressbereichs, aus welchem der DHCP Server Adressen vergibt. Die IP-Adresse muss in dem Bereich des lokalen Netzwerks liegen (siehe Abschnitt IP Interfaces).

Dieser Parameter ist zwingend erforderlich, wenn Active auf **Yes** steht.

Fixed Mapping of MAC Addresses

MAC Address	IP Address		
00:03:FF:B1:2A:00	192.168.1.64	edit	delete

MAC Address = MAC-Adresse

Die MAC Adresse ist die physikalische Adresse einer Netzwerkkarte. Die MAC Adresse der Netzwerkkarte eines Clients bringen Sie mit folgenden Befehlen in Erfahrung: `ipconfig /all` in der Windows Eingabeaufforderung und `ifconfig` unter UNIX. Der DHCP Server weist dem Client mit dieser MAC Adresse die angegebene IP-Adresse zu. Das Format der MAC Adresse sind sechs Hexadezimale Bytes, welche durch Doppelpunkt getrennt sind.

Dieser Parameter ist zwingend erforderlich.

IP Address = IP-Adresse

Der DHCP Server weist dem Client diese IP-Adresse zu. Die IP-Adresse muss in dem Bereich des lokalen Netzwerks liegen.

Dieser Parameter ist zwingend erforderlich.

10.1.6 ISDN Peer Stations

Mit diesem Menü spezifizieren sie die Routingtabelle für die WAN Gegenstellen.

Peer Name	IP Address	Netmask	Telno Call	Telno Signaled	L2	L3	Idle	Use NAT	BOD	Call-back	IP-Table	PPP Section
-----------	------------	---------	------------	----------------	----	----	------	---------	-----	-----------	----------	-------------

arcor	0.0.0.0	0.0.0.0	0010700192070	-	5	0	-1	Yes	No	-1	FWinternet	ppparcor
multi15	192.168.3.15	255.255.255.255	36	36	0	0	60	No	No	-1	SYSTEM	pppdefa
multi19	192.168.3.19	255.255.255.255	47	47	5	0	-1	No	No	-1	SYSTEM	pppm19

Peer Name

Symbolischer Abschnittsname. Dieser Name muß in der Konfiguration eindeutig sein.

IP Address

IP-Nummer der Gegenstelle. Beachten Sie auch das Kapitel Besondere Adressen.

Netmask

Netzmaske für die Gegenstelle in Punktschreibweise. Geben Sie 0.0.0.0 an, wenn Sie die Defaultroute spezifizieren.

Die Standardeinstellung beträgt 255.255.255.0.

Telno Call

Telefonnummer der Gegenstelle (Called Party Number) für abgehende Rufe, evtl. inklusive Amtsholung.

Wenn kein Dialout durchgeführt werden soll, kann der Parameter leer bleiben.

Telno Signaled

Anhand der von ISDN signalisierten Rufnummer der Gegenstelle (Calling Party Number) wird bei ankommenden Rufen die Gegenstelle identifiziert und authentisiert. Ein Stern (*) kann als Standardverbindung für eingehende Rufe verwendet werden. Folgen dem Stern weitere Ziffern, dann wird die signalisierte Rufnummer von hinten mit der Ziffernfolge verglichen (Postfix Vergleich).

Wenn keine Rufe angenommen werden sollen, kann als Parameter ein Minuszeichen (-) angegeben werden.

L2

B Kanal Schicht 2 Protokoll. PPP wird bei CAPI 2.0 über die Nummer 5 ausgewählt.

Die Standardeinstellung beträgt 0.

L3

B Kanal Schicht 3 Protokoll. Die Nummer 0 entspricht der transparenten Schicht 3 bei der CAPI 2.0.

Die Standardeinstellung beträgt 0.

Idle

Anzahl von Sekunden nach denen die Verbindung bei Inaktivität abgebaut wird.

Der Wert -2 bedeutet, daß die Voreinstellung aus dem Abschnitt [ISDND], siehe Kapitel 10.2 Konfigurationsdateien, verwendet wird.

Der Wert -1 bedeutet, daß die Verbindung niemals wegen Inaktivität abgebaut wird.

Die Standardeinstellung beträgt -2.

Use NAT

Gibt an, ob Network Address Translation durchgeführt werden soll. Diese Option ist nur sinnvoll, wenn über PPP eine IP-Nummer für die eigene Station ausgehandelt wird.

Die Standardeinstellung beträgt *No*.

BOD

Gibt an, ob bei Bedarf eine Kanalbündelung (Bandwidth On Demand) vorgenommen werden soll.

Die Standardeinstellung beträgt *No*.

Callback

Gibt die Zeit in Sekunden an, die gewartet wird, bis die Gegenstelle zurückgerufen wird. Siehe auch Kapitel 6.11, Callback. Der Wert -1 bedeutet keinen Rückruf.

Die Standardeinstellung beträgt -1.

IP-Table

Legt die für diese Verbindung geltenden Firewallregeln fest. Siehe auch Kapitel 7 Firewall-Mechanismus.

Die Standardeinstellung ist *SYSTEM*.

PPP Section

Symbolischer Name des Abschnitts für PPP Parameter.

Der Parameter kann leer bleiben, wenn kein PPP benötigt wird.

10.1.7 PPP Sections

Ein PPP Abschnitt definiert die Parameter für eine Verbindung mit Point-to-Point-Protokoll. Ein Abschnitt kann von verschiedenen Gegenstellen (Peer Stations) referenziert werden. Dies ist sinnvoll, wenn viele Gegenstellen zu spezifizieren sind, die alle die gleichen Parameter benutzen.

Section Name	LCP Section	IPCP Section	CHAP Section		
pppdefault	lcpdefault	ipcpdefault	chapdefault	edit	delete
pppm19	lcpm19	ipcpm19	chapm19	edit	delete
ppparcor	lcpdefault	ipcparcor	chaparcor	edit	delete

Section Name

Abschnittsname für PPP Parameter. Dieser Name muß in der Konfiguration eindeutig sein.

LCP Section

Symbolischer Name des Abschnitts für Link Control Protocol Parameter.

Der Parameter kann leer bleiben, wenn nur Standardeinstellungen für LCP benötigt werden.

IPCP Section

Symbolischer Name des Abschnitts für Internet Control Protocol Parameter.

Der Parameter kann leer bleiben, wenn nur Standardeinstellungen für IPCP benötigt werden.

CHAP Section

Symbolischer Name des Abschnitts für Authentisierungsprotokolle.

Der Parameter kann leer bleiben, wenn keine Authentisierung durchgeführt werden soll.

10.1.8 LCP Sections

Ein LCP Abschnitt definiert die Parameter für das Link Control Protokoll. Ein Abschnitt kann von verschiedenen PPP Abschnitten referenziert werden. Dies ist sinnvoll, wenn mehrere Gegenstellen zu spezifizieren sind, die alle die gleichen Parameter benutzen.

Section Name	Callback	Callback Type	Callback ID	AF/CF Compression	PF Compression		
lcpdefault	No	User authentication		No	No	edit	delete
lcpm19	Incoming	User authentication		Yes	Yes	edit	delete

Section Name

Abschnittsname für LCP Parameter. Dieser Name muß in der Konfiguration eindeutig sein.

Callback

Gibt den LCP Callback Modus an. Siehe Kapitel 6.11, Callback.

Callback Type

Gibt den LCP Callback Typ an. Siehe Kapitel 6.11, Callback.

Callback ID

Gibt die LCP Callback Identifikation an. Siehe Kapitel 6.11, Callback.

AF/CF Compression

Verhandlung der Adress- und Kontrollfeld-Kompression des LCP-Protokolls. Nur wenn beide Partner die Kompression wünschen, wird sie durchgeführt.

Die Standardeinstellung beträgt *No*.

PF Compression

Verhandlung der Protokollfeld Kompression des LCP-Protokolls. Nur wenn beide Partner die Kompression wünschen, wird sie durchgeführt.

Die Standardeinstellung beträgt *No*.

10.1.9 IPCP Sections

Ein IPCP Abschnitt definiert die Parameter für das Internet Protocol Control Protokoll. Ein Abschnitt kann von verschiedenen PPP Abschnitten

referenziert werden. Dies ist sinnvoll, wenn mehrere Gegenstellen zu spezifizieren sind, die alle die gleichen Parameter benutzen.

Section Name	Own IP	Remote IP	VJ compression	VJ max state	VJ compress slot ID		
ipcpdefault	210.21.3.56	0.0.0.0	No	16	No	edit	delete
ipcparcor	0.0.0.0	0.0.0.0	Yes	16	Yes	edit	delete
ipcpm19	210.21.3.56	210.21.3.19	Yes	16	Yes	edit	delete

Section Name

Abschnittsname für IPCP Parameter. Dieser Name muß in der Konfiguration eindeutig sein.

Own IP

Diese IP-Nummer wird der Gegenstelle als eigene IP-Nummer mitgeteilt. Falls die Gegenstelle dynamische IP-Nummern vergeben kann, dann kann *0.0.0.0* angegeben werden. Die Gegenstelle wird dann eine dynamische IP-Nummer zuweisen. Die ausgehandelte Nummer wird bei der Verwendung von NAT in jedem abgehenden IP Paket als Source IP-Nummer eingetragen.

Die Standardeinstellung beträgt *isdnd.cfg [INTERFACES] mif* (die IP-Nummer der *mif*-Schnittstelle).

Remote IP

IP-Nummer der Gegenstelle. Wird hier eine *0* angegeben, dann wird erwartet, daß die Gegenstelle ihre eigene IP-Nummer kennt und uns mitteilt. Falls die Gegenstelle eine IP-Nummer zugeteilt bekommen soll, muß hier die zuzuteilende IP-Adresse angegeben werden.

Die Standardeinstellung ist leer, d.h. *0.0.0.0*.

VJ compression

VanJacobsen Kompression des IP-Paketkopfes verhandeln. Nur wenn beide Partner die Kompression wünschen, wird sie durchgeführt. Mit dieser Kompression kann der Durchsatz wesentlich verbessert werden, wenn in kurzer Zeit viele kleine IP-Pakete übertragen werden.

Die Standardeinstellung beträgt *y*.

10.1.10 CHAP Sections

Ein Authentisierungsabschnitt definiert die Parameter für die Authentisierungsprotokolle CHAP (Challenging Handshake Protocol) und

PAP (Password Authentication Protocol). Ein Abschnitt kann von verschiedenen PPP Abschnitten referenziert werden. Dies ist sinnvoll, wenn mehrere Gegenstellen zu spezifizieren sind, die alle die gleichen Parameter benutzen.

Section Name	Authentication	Local username	Local password	Remote username	Remote password		
chapdefault	No					edit	delete
chaparcor	CHAP	arcor			internet	edit	delete
chapm19	CHAP		winnt	Administrator		edit	delete

Section Name

Abschnittsname für CHAP Parameter. Dieser Name muß in der Konfiguration eindeutig sein.

Authentication

Dieser Parameter gibt an, welches Authentisierungsverfahren verwendet werden soll.

Einer der folgenden Parameter kann ausgewählt werden:

No, PAP, CHAP, CHAP or PAP

Wenn *CHAP or PAP* ausgewählt ist, dann hat das CHAP-Verfahren Vorrang.

Die Standardeinstellung beträgt *CHAP or PAP*.

Local username

Diese Zeichenkette wird verwendet, um die lokale Station bei der Gegenstelle zu identifizieren.

Wenn die Zeichenkette leer ist, dann erfolgt keine Anmeldung.

Local password

Diese Zeichenkette erwartet die lokale Station als Kennwort von der Gegenstelle.

Wenn die Zeichenkette leer ist, wird die Identifikation der Gegenstelle nicht erwartet.

Remote username

Diese Zeichenkette erwartet die lokale Station von der Gegenstelle als Identifikation. Falls die Identifikation nicht übereinstimmt, kommt die Verbindung nicht zustande.

Wenn die Zeichenkette leer ist, wird die Identifikation der Gegenstelle nicht überprüft.

Remote password

Diese Zeichenkette wird als Kennwort für die Anmeldung der lokalen Station bei der Gegenstelle verwendet.

Wenn die Zeichenkette leer ist, erfolgt keine Anmeldung.

10.1.11 IP-Tables (Firewall)

Siehe Kapitel 7 Firewall-Mechanismus.

10.1.12 Port Forwarding

Port Forwarding dient dazu, Dienste aus dem privaten Netz für Internetrechner verfügbar zu machen, wie z. B. ein Webserver oder eine Webcam.

Dabei ist zu beachten, dass der lokale Rechner, welcher diesen Dienst anbietet auf dem entsprechenden Port (z. B. Port 80 bei einem Webserver) potentiell Angriffen aus dem Internet ausgesetzt ist. Durch Port Forwarding wird der Schutz vor direkten Angriffen aus dem Internet aufgehoben.

Konfigurationsänderungen werden erst nach einem (erneuten) Internet Verbindungsaufbau wirksam.

IP Address	TCP Ports	UDP Ports	Description		
192.168.1.32	80		Webserver	edit	delete
192.168.1.33		500,4500	IPSec Gateway	edit	delete

IP Address

Die IP-Adresse des Rechners aus dem lokalen, privaten Netz, welcher aus dem Internet erreichbar sein soll. Die IP-Adresse muss in dem Bereich des lokalen Netzwerks liegen (siehe Abschnitt IP Interfaces).

Dieser Parameter ist zwingend erforderlich.

TCP Ports

Die TCP-Dienst-Adresse(n), welche aus dem Internet erreichbar sein soll(en). Sie können eine Liste oder auch einen Bereich von Portnummern angeben (siehe auch Kapitel 7.7 Portdefinition).

Dieser Parameter ist zwingend erforderlich.

UDP Ports

Die UDP-Dienst-Adresse(n), welche aus dem Internet erreichbar sein soll(en). Sie können eine Liste oder auch einen Bereich von Portnummern angeben (siehe auch Kapitel 7.7 Portdefinition).

Dieser Parameter ist zwingend erforderlich.

Description

Die Beschreibung dient lediglich Dokumentationszwecken.

10.1.13 IPsec and VPN

Siehe Kapitel 8 IPsec und VPN

10.1.14 DynDNS

Siehe Kapitel 8 IPsec und VPN

10.1.15 Show active ISDN/DSL Connections

Dieser Menüpunkte zeigt Ihnen eine Liste der aktiven WAN-Verbindungen. Einzelne Verbindungen können gezielt abgebaut werden.

WAN Connections

Start time	Direction	Source IP	Dest. IP	NAT IP	Telno	State	Release	RX-Bytes	TX-Bytes
20.02.2002 11:01:36	OUT	210.21.1.41	194.25.2.129	84.138.235.69	0191011	Data	38	54014	2983

Start time

Datum und Uhrzeit des Aufbaus der Verbindung

Direction

Ankommende (IN) oder abgehende Verbindung (OUT)

Source IP / Dest. IP

Source und Destination IP des IP-Pakets, das den Verbindungsaufbau gestartet hat

NAT IP

Bei Internetverbindung ist die öffentliche IP Adresse des Routers.

Telno

Telefonnummer der Gegenstelle. Bei einem externen Modem am Port P1 wird pppoe angezeigt. Bei einem externen Modem an einem der Ports P2 bis P6 wird pppoe-lan angezeigt.

State

Der Zustand der Verbindung. Hier kann man erkennen, ob der Router die WAN-Verbindung gerade aufbaut oder ob die Verbindung bereits aufgebaut ist oder abgebaut wird

Release

Die Zeit in Sekunden, bis der Router die Verbindung wegen Nichtaktivität trennt. Bei der Konfiguration "Always On", d. h. -3 als Idle Wert, steht hier **never**.

RX-Bytes / TX-Bytes

Anzahl der empfangenen bzw. gesendeten Bytes

10.1.16 Show active TCP/UDP/ICMP Connections

Mittels dieses Menüpunktes können Sie sich Listen der aktiven TCP-, UDP- und ICMP-Verbindungen ausgeben.

TCP Connections

Source IP	Dest. IP	Source Port	Dest. Port	State	Timeout (sec)
210.21.41	194.25.2.129	1104	7705	SYN_SENT	61
210.21.41	194.25.2.129	1105	7705	SYN_SENT	88

UDP Connections

Source IP	Dest. IP	Source Port	Dest. Port	Timeout (sec)
-----------	----------	-------------	------------	---------------

ICMP Connections

Source IP	Dest. IP	Type	Code	Id	Timeout (sec)
210.21.41	194.25.2.129	8	0	256	20

Source IP / Dest. IP

Source und Destination IP
bei NAT-Verbindungen wird die zugewiesene IP angegeben

Source Port / Dest. Port

Source und Destination Port
bei NAT-Verbindungen wird der gemappte Port angegeben

State

TCP Zustand

Timeout

verbleibende Zeit bis diese Verbindung gelöscht wird, wenn kein anderes Ereignis wie Zustandswechsel oder Paketempfang eintritt.

Type / Code / Id

Anzeige der ICMP Header-Felder Type, Code und Identifier

10.1.17 Show Logfile

Mit diesem Menüpunkt wird die Datei isdnd.log entsprechend dem in Kapitel 4.14 Log-Datei beschriebenen Format dargestellt.

10.1.18 Update Router Image

Bei Anwahl des Menüpunktes Update Router Image erscheint ein Formular mit Eingabefeld und einem optionalen Dateidialog, der die Auswahl einer

Datei (Routerimage im tar-Format) von dem lokalen System erlaubt. Durch Betätigung des Aktionsknopf **Upload** wird die Datei über einen Standardmechanismus des HTTP (Post Methode) zum Router übertragen. Im gleichen Menü erlaubt nach Auswahl der Datei im Feld **Flash TAR File** der Aktionsknopf **Flash** das Brennen der übertragenen Datei. Der Erfolg bzw. Misserfolg jeder Aktion wird dem Web-Browser zurückgemeldet.

Der Dateidialog in Verbindung mit der Post Methode wird ab Netscape V3.01 und ab Internet Explorer V4.0 unterstützt.

10.1.19 Trace Parameters

Dieses Menü wird nur zur Fehlerdiagnose benötigt und dient dazu, die Trace Parameter für den hlogger bzw. für den Web-Trace einzustellen und evtl. den Web-Trace zu starten. Die Funktionalität des Web-Trace entspricht dem Starten des gpf2 Programmes (siehe Kapitel 11.2.3 gpf2). Der hlogger erlaubt die Aufzeichnung von Trace/Log-Informationen des Routers auf einem Server (WindowsNT/2000 oder Linux).

Wird das Eingabefeld **Log to server** auf yes gesetzt, so wird die Aufzeichnung mittels hlogger gestartet. Das Feld **Logserver IP** gibt die IP-Adresse des Rechners an, auf dem der hlogger läuft.

Das Eingabefeld **Channels** bestimmt die Kanäle, die aufgezeichnet werden sollen. Dabei wird der angegebene Wert als Bitmaske interpretiert, deren Bits den einzelnen Kanälen entsprechen:

Channels	B2	B1	D-Kanal
0			
1			o
2		o	
3		o	o
4	o		
5	o		o
6	o	o	
7	o	o	o

Das Eingabefeld **Debug** legt fest, welche Debug-Informationen aus dem ISDN Protokollstack ausgegeben werden sollen (siehe auch Anhang B.4).

Der Aktionsknopf **Set parameters** setzt die Trace Parameter, während mit dem Aktionsknopf **Trace now to browser** die Trace-Ausgabe auf den Browser gestartet wird.

10.2 Konfigurationsdateien

Die Datei *isdnd.cfg* enthält mehrere Abschnitte, die jeweils aus einer Gruppe zusammengehörender Parameter bestehen. Ein Abschnitt beginnt mit einem Abschnittsnamen. Abschnittsnamen werden in eckige Klammern gesetzt [Abschnitt]. Ein Abschnitt erstreckt sich bis zum Anfang des darauf folgenden Abschnitts oder, im Fall des letzten Abschnitts, bis zum Dateiende. Innerhalb eines Abschnitts finden sich Eintragungen des Typs:

Parameter = Wert

Wert kann hierbei eine Zeichenfolge oder eine Ganzzahl sein; hexadezimale Notation ist ebenfalls zulässig. Falls die Zeichenfolge Leerzeichen enthält, muß sie in doppelte Hochkomma eingeschlossen werden ("Wert mit Leerzeichen").

10.2.1 Abschnitt [ISDND]

Dieser Abschnitt erlaubt allgemeine Einstellungen des Routers.

MSN = Nummer

Nummer gibt die MSN (Multiple Subscriber Number, Mehrfachrufnummer) an, die das ISDN Gerät von anderen ebenfalls angeschlossenen Geräten oder Softwareprogrammen unterscheidet. Die letzten Ziffern der Nummer, welche durch Ihre Nebenstellenanlage/Vermittlungsstelle als Rufnummer des Angerufenen (Called Party Number) signalisiert wird, wird mit der angegebenen MSN verglichen. Bei Gleichheit wird der Ruf angenommen, sonst wird er ignoriert, damit ein anderes Endgerät die Möglichkeit hat, den Ruf anzunehmen. Ist die Nummer nicht angegeben (leeres Eingabefeld), dann wird der MSN Vergleich nicht durchgeführt und der Ruf immer angenommen. Bei abgehenden Rufen teilt HERMES die MSN der Nebenstellenanlage/Vermittlungsstelle als eigene Nummer mit (Calling Party Number).

Das Dienstmerkmal *Subadressing* wird z.Zt. nicht unterstützt.

Standardeinstellung: 1

MSNWakeupSignal = Nummer

Nummer gibt die MSN an, die bei ankommenden Rufen mit der Rufnummer des Angerufenen (Called Party Number) verglichen wird.

Wenn die letzten Ziffern übereinstimmen, wird das Signal RI der V.24-Schnittstelle für 100ms aktiviert. Hiermit kann z. B. eine USV bzw. ein Server ferngesteuert eingeschaltet werden. Auf die Rufannahme hat diese Funktionalität keine Auswirkung. Insbesondere kann `MSNWakeupSignal` gleich `MSN` sein. Mit `unset` kann diese Funktion deaktiviert werden.

Standardeinstellung: `unset`

ARDInterval = Wert

Wert gibt die Dauer des überwachten Zeitintervalls in Einheiten von Stunden an. Der Wert -1 schaltet die Überprüfung aller Grenzwerte aus.

Standardeinstellung: -1

ARDCharge = Wert

Wert gibt die Summe der signalisierten Gebühreneinheiten an. Falls Gebühren in nationaler Währung signalisiert werden, werden diese z.Zt. ignoriert. Der Wert -1 schaltet die Überprüfung dieses Grenzwertes aus.

Standardeinstellung: -1

ARDCount = Wert

Wert gibt die Anzahl der abgehenden Verbindungen an. Der Wert -1 schaltet die Überprüfung dieses Grenzwertes aus.

Standardeinstellung: -1

ARDDuration = Wert

Wert gibt die Summe der Verbindungszeiten für abgehende Verbindungen in Minuten an. Der Wert -1 schaltet die Überprüfung dieses Grenzwertes aus.

Standardeinstellung: -1

ConfPort = Wert

Wert gibt an, unter welcher Nummer die HTTP-Schnittstelle zur Konfiguration (Web-Browser-Schnittstelle) erreichbar ist. Der Standardwert ist 7705. Dies ist eine freie Portnummer, die von beliebigen Programmen benutzt werden darf. HTTP-Server verwenden normalerweise den zugewiesenen Port 80; damit keine Konflikte zwischen den Programmen entstehen, wurde der freie Port 7705 verwendet. Die Änderung der Portnummer wird erst nach Neustart wirksam.

Standardeinstellung: 7705

Timeout = Wert

Wert gibt die Haltezeit für die Verbindung in Sekunden an, siehe Kapitel 6.5, Verbindungsabbau.

Standardeinstellung: 30

JournalingPort = UDP Portnummer

Das Journaling wird über diese Konfigurationsoption aktiviert. Wenn der Eintrag fehlt oder leer ist, erzeugt isdnd keine Journaling Nachrichten. Die Portnummer für das syslog Protokoll ist 514. Die empfohlene Portnummer für eine proprietäre MULTIDATA Client/Server Kommunikation ist 7707. Weitere Hinweise zum Journaling finden sie im Journaling Handbuch.

Standardeinstellung ist leer

Debug = Liste

Liste gibt an, welche Logausgaben vorgenommen werden sollen. In Anhang B.5 sind die möglichen Einstellungen näher erläutert.

Empfohlene Einstellung: 012346

Standardeinstellung: leere Liste

LogfileSize = Wert

Wert gibt die Maximalgröße der Datei für Accounting und Logausgaben (*isdnd.log*) in Bytes an. Wenn die maximale Größe erreicht ist, dann wird die Datei in *isdnd.log.old* umbenannt und eine neue Datei *isdnd.log* angelegt.

Standardeinstellung: 30000

Logfile = Name

Name der Datei für Accounting und Logausgaben.

Standardeinstellung: *isdnd.log*

Timeserver = IP-Nummer

IP-Nummer oder symbolischer Name des Timeservers, von welchem der Router beim Start das aktuelle Datum und die Uhrzeit erfragt und als Systemzeit setzt. Ist dieses Feld leer, wird keine Einstellung des Datums und der Uhrzeit vorgenommen. Änderungen werden erst bei Neustart des Routers aktiv.

Standardeinstellung: leer

10.2.2 Abschnitt [*peer*]

Der Name dieses Abschnitts wird aus der Datei */etc/hosts* referenziert. Dort muß eine Zeile in der folgenden Form vorliegen:

```
Host      peer
```

Host ist dabei eine IP-Nummer oder ein symbolische Hostname. Folgende Parameter sind für diesen Abschnitt definiert:

PeerIP = *IP-Nummer*

IP-Nummer der Gegenstelle. Siehe auch Kapitel 6.7 Besondere Adressen.

Standardeinstellung: die IP Nummer aus der Datei */etc/hosts*.

Netmask = *Netzmaske*

Netzmaske gibt die Netzmaske für die Gegenstelle in Punktschreibweise an. Geben Sie *0.0.0.0* an, wenn Sie die Default-Route spezifizieren. Siehe auch Kapitel 6.7 Besondere Adressen.

Standardeinstellung: *255.255.255.0*

Call = *Telefonnummer*

Telefonnummer der ISDN-Gegenstelle, evtl. inklusive Amtsholung.



Für diesen Parameter gibt es besondere Werte, welche am Ende dieses Kapitels erläutert werden.

Standardeinstellung: leere Zeichenkette

Listen = *Telefonnummer*

Anhand der von ISDN signalisierten Rufnummer der Gegenstelle (Calling Party Number) wird bei ankommenden Rufen die Gegenstelle identifiziert und authentisiert. Ein Stern (*) kann als Standardverbindung für eingehende Rufe verwendet werden. Folgen dem Stern weitere Ziffern, dann wird die signalisierte Rufnummer von hinten mit der Ziffernfolge verglichen (Postfix Vergleich).

Wenn keine Rufe angenommen werden sollen, kann als Parameter ein Minuszeichen (-) angegeben werden.

Standardeinstellung: leere Zeichenkette

L1Prot = *Wert*

B Kanal Schicht 1 Protokoll. Siehe Kapitel B.2.1 Schicht 1 Protokolle.

Standardeinstellung: 0

L2Prot = Wert

B Kanal Schicht 2 Protokoll. Siehe Kapitel B.2.2 Schicht 2 Protokolle.
Standardeinstellung: 0

L3Prot = Wert

B Kanal Schicht 3 Protokoll. Siehe Kapitel B.2.3 Schicht 3 Protokolle.
Standardeinstellung: 0

Timeout = Wert

Wert gibt die Zeit in Sekunden an, nach der die Verbindung bei Inaktivität abgebaut werden. Der Wert -2 bedeutet, daß die Voreinstellung aus dem Abschnitt [ISDND] verwendet wird. Der Wert -1 bedeutet, daß die Verbindung niemals wegen Inaktivität abgebaut.

Standardeinstellung: -2

NAT = Wert

Gibt an, ob Network Address Translation durchgeführt werden soll oder nicht. Dieser Parameter wird nur ausgewertet, wenn über PPP eine IP Nummer für die eigene Seite ausgehandelt wird.

- 0 : Keine Network Address Translation
- 1 : Network Address Translation

Standardeinstellung: 0

MaxChan = Wert

Gibt die maximale Anzahl B-Kanäle an, die zu dieser Gegenstelle aufgebaut werden sollen. Siehe auch Kapitel 6.12 Kanalbündelung.

Standardeinstellung: 1

Callback = Wert

Gibt die Zeit in Sekunden an, die gewartet wird, bis die Gegenstelle zurückgerufen wird. Der Wert -1 bedeutet keinen Rückruf. Siehe auch Kapitel 6.11, Callback.

Standardeinstellung: -1

PPP = PeerPPP

Symbolischer Name des Abschnitts für PPP Parameter. Dieser Parameter ist nur relevant, wenn PPP als Protokoll eingestellt ist.

Standardeinstellung: leer

Besondere Werte für den Parameter CALL

Call = pppoe

Der Router baut eine PPPoE Verbindung über ein externes DSL Modem am **Port P1** auf. Die Parameter L1Prot., L2Port, L3Prot und MaxChan haben in diesem Fall keine Bedeutung.

Call = pppoe-lan

Der Router baut eine PPPoE Verbindung über ein externes DSL Modem an einem der **Ports P2 bis P6** auf. Die Parameter L1Prot., L2Port, L3Prot und MaxChan haben in diesem Fall keine Bedeutung.

Call = ipgw

Der Router verwendet ein externes IP-Gateway am **Port P1** (eth1).

Für eine korrekte Verbindung in das Internet müssen die Parameter PeerIP und Netmask den Wert 0.0.0.0 enthalten. NAT muss den Wert 1 enthalten. IP-Table und Timeout werden wie üblich behandelt. Die Parameter WanAddress, WanNetmask, GatewayAddress und NameserverAddress sind unten beschrieben. Alle weiteren Parameter in diesem *[peer]* Abschnitt werden ignoriert!

IP-Gateway Konfiguration

Die folgenden Parameter werden nur dann benötigt, wenn der Parameter Call den Wert **ipgw** hat. Ein IP-Gateway lässt sich auch im Menü *Configuration Assistant* konfigurieren. In diesem Untermenü erscheint der Eintrag *New Internet via IP Gateway*. Diese Option ist nur für HERMES-PRO/X verfügbar.

WanAddress = IP Adresse

Die lokale IP Adresse der WAN Schnittstelle in einer IP-Gateway Konfiguration. Falls der Parameter den Wert 0.0.0.0 enthält, dann wird er über DHCP ermittelt.



Achtung: Für die vier IP-Gateway Parameter WanAddress, WanNetmask, GatewayAddress und NameserverAddress ist eine gemischte Konfiguration (d. h. manuell und DHCP) möglich. Ein manuell konfigurierter Wert hat Vorrang vor einem Wert, welcher von einem DHCP Server geliefert wird.

Beispiel: **wanAddress = 192.168.21.10**

Standardeinstellung: **0.0.0.0**, d. h. der Parameter wird über DHCP ermittelt.

WanNetmask = Netzmaske

Die Netzmaske für die lokale WAN Schnittstelle in einer IP Gateway Konfiguration. Falls der Parameter den Wert 0.0.0.0 enthält, dann wird er über DHCP ermittelt.



Achtung: Die IP Adresse und die Netzmaske der WAN Schnittstelle dürfen nicht mit der IP Adresse und Netzmaske der LAN Schnittstelle identisch sein, da dann LAN Rechner evtl. nicht mehr erreichbar sind. Wenn die IP Adresse des Gateways eine LAN Adresse ist, dann muss als Netzmaske der Wert 255.255.255.255 verwendet werden.

Beispiel: **WanNetmask = 255.255.255.0**

Standardeinstellung: 0.0.0.0, d. h. der Parameter wird über DHCP ermittelt.

GatewayAddress = IP Adresse

Die IP Adresse des Gateways für den Internetzugang in einer IP Gateway Konfiguration. Falls der Parameter den Wert 0.0.0.0 enthält, dann wird er über DHCP ermittelt.

Beispiel: **GatewayAddress = 192.168.21.1**

Standardeinstellung: 0.0.0.0, d. h. der Parameter wird über DHCP ermittelt.

NameserverAddress = IP Adresse

Die IP Adresse des Nameservers für den Internetzugang in einer IP Gateway Konfiguration. Falls der Parameter den Wert 0.0.0.0 enthält, dann wird er über DHCP ermittelt.

Beispiel: **GatewayAddress = 192.168.21.1**

Standardeinstellung: 0.0.0.0, d. h. der Parameter wird über DHCP ermittelt.

10.2.3 Abschnitt [peerPPP]

Dieser Abschnitt definiert die Parameter für eine Verbindung mit Point-to-Point-Protokoll. Ein Abschnitt kann von verschiedenen Gegenstellen (Peer Stations) referenziert werden. Dies ist sinnvoll, wenn viele Gegenstellen zu spezifizieren sind, die alle die gleichen Parameter benutzen.

LCP = Name

Symbolischer Name des Abschnitts für Link Control Protocol Parameter. Der Parameter kann leer bleiben, wenn nur Standardeinstellungen für LCP benötigt werden.

Standardeinstellung: leer

IPCP = *Name*

Symbolischer Name des Abschnitts für Internet Control Protocol Parameter. Der Parameter kann leer bleiben, wenn nur Standardeinstellungen für IPCP benötigt werden.

Standardeinstellung: leer

CHAP = *Name*

Symbolischer Name des Abschnitts für Authentisierungsprotokolle. Der Parameter kann leer bleiben, wenn keine Authentisierung durchgeführt werden soll.

Standardeinstellung: leer

10.2.4 Abschnitt [PeerLCP]

Dieser Abschnitt definiert die Parameter für das Link Control Protokoll. Ein Abschnitt kann von verschiedenen PPP Abschnitten referenziert werden. Dies ist sinnvoll, wenn mehrere Gegenstellen zu spezifizieren sind, die alle die gleichen Parameter benutzen.

CallbackMode = *Wert*

Gibt den LCP Callback Modus an. Siehe auch Kapitel 6.11, Callback.

0 : No
4 : Incoming
8 : Outgoing
12 : InOut

Standardeinstellung: 0

CallbackType = *Wert*

Gibt den LCP Callback Type an. Dieser Parameter ist nur von Bedeutung, wenn Callbackmode einen Wert ungleich 0 hat. Siehe auch Kapitel 6.11, Callback.

Standardeinstellung: 0

CallbackID = *Zeichenkette*

Gibt die LCP Callback Identifikation an. Siehe auch Kapitel 6.11, Callback.

Standardeinstellung: leer

AddrContrField = [y|n]

Verhandlung der Adreß- und Kontrollfeld-Kompression des LCP-Protokolls. Nur wenn beide Partner die Kompression wünschen, dann wird sie durchgeführt.

Standardeinstellung: n

ProtocolField = [y|n]

Verhandlung der Protokollfeld Kompression des LCP-Protokolls. Nur wenn beide Partner die Kompression wünschen, dann wird sie durchgeführt.

Standardeinstellung n

10.2.5 Abschnitt [peerIPCP]

Dieser Abschnitt definiert die Parameter für das Internet Protocol Control Protokoll. Ein Abschnitt kann von verschiedenen PPP Abschnitten referenziert werden. Dies ist sinnvoll, wenn mehrere Gegenstellen zu spezifizieren sind, die alle die gleichen Parameter benutzen.

OwnIP = Wert

Wert wird der Gegenstelle als eigene IP-Nummer mitgeteilt. Falls die Gegenstelle dynamische IP-Nummern vergeben kann, dann kann 0.0.0.0 angegeben werden, damit HERMES-PRO/X von der Gegenstelle eine dynamische IP-Nummer zugewiesen bekommt. Die ausgehandelte Nummer wird bei der Verwendung von NAT in jedem abgehenden IP Paket als Source IP Nummer eingetragen.

Standardeinstellung: Die IP Nummer der mit Schnittstelle

RemIP = Wert

IP-Nummer der Gegenstelle. Wird hier 0.0.0.0 angegeben, dann wird erwartet, daß die Gegenstelle ihre eigene IP-Nummer kennt und uns mitteilt. Falls die Gegenstelle eine IP-Nummer zugeteilt bekommen soll, dann muß hier die zuzuteilende IP-Adresse angegeben werden.

Standardeinstellung: 0.0.0.0

VJ = [y|n]

VanJacobsen Kompression des IP-Paketkopfes. Nur wenn beide Partner die Kompression wünschen, wird sie durchgeführt. Mit dieser

Kompression kann der Durchsatz wesentlich verbessert werden, wenn in kurzer Zeit viele kleine IP-Pakete übertragen werden.

Standardeinstellung: γ

10.2.6 Abschnitt [peerCHAP]

Ein Authentisierungsabschnitt definiert die Parameter für die Authentisierungsprotokolle CHAP (Challenging Handshake Protocol) und PAP (Password Authentication Protocol). Ein Abschnitt kann von verschiedenen PPP Abschnitten referenziert werden. Dies ist sinnvoll, wenn mehrere Gegenstellen zu spezifizieren sind, die alle die gleichen Parameter benutzen.

LocalName = Name

Name wird verwendet, um die lokale Station bei der Gegenstelle zu identifizieren. Wenn kein Name angegeben wurde, dann erfolgt keine Anmeldung.

Standardeinstellung: leer

LocalPassword = Zeichenkette

Diese Zeichenkette erwartet die lokale Station als Kennwort von der Gegenstelle. Wenn die Zeichenkette leer ist, dann wird die Identifikation der Gegenstelle nicht erwartet.

Standardeinstellung: leer

RemoteName = Zeichenkette

Diese Zeichenkette erwartet die lokale Station von der Gegenstelle als Identifikation. Falls die Identifikation nicht übereinstimmt, dann kommt die Verbindung nicht zustande. Wenn die Zeichenkette leer ist, dann wird die Identifikation der Gegenstelle nicht überprüft.

Standardeinstellung: leer

RemotePassword = Zeichenkette

Diese Zeichenkette wird als Kennwort für die Anmeldung der lokalen Station bei der Gegenstelle verwendet. Wenn die Zeichenkette leer ist, dann erfolgt keine Anmeldung.

Standardeinstellung: leer

Protocol = Wert

Dieser Parameter gibt an, welches Authentisierungsverfahren verwendet werden soll. Wenn *CHAP* or *PAP* ausgewählt ist, dann hat das CHAP-

Verfahren Vorrang, d.h. CHAP wird verwendet, wenn beide Seiten CHAP unterstützen.

- 0 : No
- 1 : CHAP
- 2 : PAP
- 3 : CHAP or PAP

Standardeinstellung: 3 (CHAP or PAP).

10.2.7 Abschnitt [INTERFACES]

EtherMode = [10|100]

Dieser Parameter ist veraltet und wird nicht mehr ausgewertet.

Standardeinstellung 10

fec0 = *IP-Nummer*

Nummer gibt die IP-Nummer der Ethernetschnittstelle an.

Standardeinstellung 192.168.2.1

fec0mask = *IP-Nummer*

Nummer gibt die Netzmaske für die Ethernetschnittstelle an.

Standardeinstellung: 255.255.255.0

mif = *IP-Nummer*

Nummer gibt die IP-Nummer an, unter der die IP-Schicht von HERMES-PRO/X über ISDN erreichbar ist.

Standardeinstellung: 192.168.3.1

isdnd = *IP-Nummer*

Nummer gibt die IP-Nummer an, unter welcher der Prozeß *isdnd* erreichbar ist. Diese IP-Nummer ist zur Zeit nicht von Bedeutung.

10.2.8 Abschnitt [DHCPRange]

Der DHCP Server weist Clients eine IP-Adresse aus einem konfigurierbaren Bereich zu.

Active = Yes | No

Dieser Parameter aktiviert den DHCP Server, wenn der Wert auf **Yes** steht. Beim Wert **No** ist der DHCP Server deaktiv. Eine Änderung hat sofortige Auswirkung.

Die Standardeinstellung beträgt **No**

Start = IP-Adresse

Dies ist die erste Adresse eines Adressbereichs, aus welchem der DHCP Server Adressen vergibt. Die IP-Adresse muss in dem Bereich des lokalen Netzwerks liegen.

Dieser Parameter ist zwingend erforderlich, wenn Active auf **Yes** steht.

End = IP-Adresse

Dies ist die letzte Adresse eines Adressbereichs, aus welchem der DHCP Server Adressen vergibt. Die IP-Adresse muss in dem Bereich des lokalen Netzwerks liegen.

Dieser Parameter ist zwingend erforderlich, wenn Active auf **Yes** steht.

10.2.9 Abschnitt [DHCPMapping n]

Der DHCP Server kann eine direkte Zuordnung der MAC Adresse zu einer IP-Adresse vornehmen. Die Abschnittsnamen müssen von 1 beginnend, aufsteigend nummeriert sein.

Beispiel:

```
[DHCPMapping1]
MACAddress = "00:03:FF:B0:2A:00"
IPAddress  = "192.168.1.64"
```

```
[DHCPMapping1]
MACAddress = "08:00:46:B1:2A:D3"
IPAddress  = "192.168.1.65"
```

MACAddress = MAC-Adresse

Die MAC Adresse ist die physikalische Adresse einer Netzwerkkarte. Die MAC Adresse der Netzwerkkarte eines Clients bringen Sie mit folgenden Befehlen in Erfahrung: `ipconfig /all` in der Windows Eingabeaufforderung und `ifconfig` unter UNIX. Der DHCP Server weist dem

Client mit dieser MAC Adresse die angegebene IP-Adresse zu. Das Format der MAC Adresse sind sechs Hexadezimale Bytes, welche durch Doppelpunkt getrennt sind.

Dieser Parameter ist zwingend erforderlich.

IPAddress = *IP-Adresse*

Der DHCP Server weist dem Client diese IP-Adresse zu. Die IP-Adresse muss in dem Bereich des lokalen Netzwerks liegen.

Dieser Parameter ist zwingend erforderlich.

10.2.10 Abschnitt [*PortForwarding*]

Die Abschnittsnamen müssen von 1 beginnend, aufsteigend nummeriert sein.

DstIP = *IP-Adresse*

Die IP-Adresse des Rechners aus dem lokalen, privaten Netz, welcher aus dem Internet erreichbar sein soll. Die IP-Adresse muss in dem Bereich des lokalen Netzwerks liegen (siehe Abschnitt IP Interfaces).

Dieser Parameter ist zwingend erforderlich.

TCPPorts = *Portliste*

Die TCP-Dienst-Adresse(n), welche aus dem Internet erreichbar sein soll(en). Sie können eine Liste oder auch einen Bereich von Portnummern angeben (siehe auch Kapitel 7.7 Portdefinition).

Dieser Parameter ist zwingend erforderlich.

UDPPorts = *Portliste*

Die UDP-Dienst-Adresse(n), welche aus dem Internet erreichbar sein soll(en). Sie können eine Liste oder auch einen Bereich von Portnummern angeben (siehe auch Kapitel 7.7 Portdefinition).

Dieser Parameter ist zwingend erforderlich.

Description = "*Beschreibung*"

Die Beschreibung dient lediglich Dokumentationszwecken.

10.2.11 Abschnitt [TRACE]

LogToServer = [yes|no]

Aktiviert die Aufzeichnung von Log/Trace-Informationen über den hlogger. Siehe auch Dokumentation Dienstprogramm hlogger.

Standardeinstellung: no

LogServer = *IP-Nummer*

IP-Nummer des Servers auf dem hlogger läuft.

Standardeinstellung: leer

Channels = *Wert*

Bestimmt die Kanäle, die aufgezeichnet werden sollen.

D-Kanal: 0x01, B-Kanal 1: 0x02, B-Kanal 2: 0x04

Standardeinstellung: 0

Debug = *Wert*

Schaltet Debug-Informationen aus dem ISDN Protokollstack ein. Siehe auch Anhang B.4 Debug-Informationen.

Standardeinstellung: 0

11 Betriebssystem des Routers

Das Betriebssystem und die Konfigurationsdaten von HERMES-PRO/X liegen zunächst in einem nichtflüchtigen Speicher (4 MByte Flash-ROM) in komprimierter Form (Routerimage) vor. Beim Startvorgang wird das Betriebssystem in den Hauptspeicher (16 MByte RAM) entpackt und gestartet. Die Konfigurationsdaten werden beim Start des Betriebssystems als Dateien in das RAM Filesystem kopiert.

HERMES-PRO/X läuft unter dem Betriebssystem Linux mit den folgenden Eigenschaften:

- Multitasking und Multiuser Fähigkeit
- RAM Filesystem
- TCP/IP Stack
- NFS

Sie können sich sowohl über die V.24 Schnittstelle als auch mit Hilfe eines Telnet Clients über eine Netzwerkschnittstelle (Ethernet oder ISDN) einloggen.

11.1 Leistungsumfang

Werksseitig ist der Benutzer *root* mit dem Kennwort *HERMES* definiert. Mit dem Kommando `passwd` kann das Kennwort geändert werden. Soll das neue Kennwort permanent gespeichert werden, muß die Kommandozeile

```
flash_tool -w /etc/passwd
```

ausgeführt werden.

Folgende Programme sind im Verzeichnis */bin* vorhanden:

Beschreibung	Kommando
Dateiverwaltung	ls, cp, rm, mv, chmod, mkdir, df
Anzeige	cat, echo, less, more
Allgemein	bash (Shell), ps, date, hostname, passwd, printenv, reboot
Netzwerk	ifconfig, ping, route, unfsio (NFS), mount, umount
Serverdienste	inetd, fingerd, telnetd, ftpd
Tools	vi, flash_tool, getcfg

Tab. 1: Betriebssystemkommandos

Zusätzliche Programme befinden sich im Verzeichnis */usr/lib/hermes*:

Beschreibung	Kommando
HERMES Tools	hcmd, testhsc, gpf2, fppp, fascii, setup
Serverdienste	isdnd, rcapid

Tab. 2: Router spezifische Kommandos

Zugriff auf den FTP-Server:

Auf den FTP-Server kann über jede Netzwerkschnittstelle zugegriffen werden. Der (Lese-)Zugriff mit Hilfe eines Web-Browsers ist ebenfalls möglich.

Flash-ROM:

Das Flash-ROM enthält folgende Dateien:

Datei	Beschreibung
ppcboot	Bootlader, max. 128Kbyte
pMulti	Komprimiertes Routerimage, max. 3840 Kbyte
a, b, c	Konfigurationsbereich, max 128 Kbyte

In dem Konfigurationsbereich können viele Konfigurationsdateien permanent gespeichert werden. Neben den vom Routingprozeß benötigten Dateien */usr/lib/hermes/isdnd.cfg*, */etc/hosts* und */etc/ihosts* kann z.B. auch eine Benutzer-eigene */etc/passwd* dort gespeichert werden. Beim Aktualisieren des Routerimages bleiben die Konfigurationsdaten erhalten. Die Schreib- und Leseoperationen auf dem Flash-ROM erfolgt mit dem Kommando *flash_tool*.

11.2 HERMES-spezifische Hilfsprogramme

11.2.1 flash_tool

Das Programm *flash_tool* dient dazu, den Flash Speicher des Routers zu schreiben und zu lesen.

Parameter:

- r** *Datei*
Datei aus dem Flash Speicher lesen. Der Dateiname muß vollständig mit Pfad angegeben werden.
- w** *Datei*
Datei in den Flash Speicher schreiben. Der Dateiname muß vollständig mit Pfad angegeben werden.
- d** *Datei*
Datei aus dem Flash Speicher löschen. Der Dateiname muß vollständig mit Pfad angegeben werden.
- l**
Alle Dateien anzeigen, die sich im Flash Speicher befinden.
- i** *Datei c3po*
Schreiben des Routerimages.
- b** *Datei c3po*
Schreiben des Bootladers.
- t** *Datei*
Um keine Verwechslungen zuzulassen (z.B. defektes Routerimage schreiben, Tippfehler, etc.) lässt diese Option ein **tar-Archiv** als Quelle zum beschreiben des Flash-Speichers zu. In das Archiv können eine oder auch mehrere Dateien eingepackt sein. So kann sichergestellt werden, daß der Bootlader, das Routerimage und die Konfigurationsdateien konsistent bleiben.

Wenn das tar-Archiv eine Datei mit den Namen **router.image.gz** enthält, dann wird sie als Routerimage gebrannt.

Wenn das tar-Archiv eine Datei mit den Namen **loader** enthält, dann wird sie als Bootlader gebrannt.

Andere Dateien brennt `flash_tool` als Konfigurationsdatei und stellt vor dem Schreiben sicher, daß keine anderen Dateien überschrieben werden.

-P

Ausgeben der Seriennummer. Dieser Parameter wird unter Linux nicht unterstützt. Bitte verwenden Sie unter Linux das Kommando `printenv`.

11.2.2 testhsc

`testhsc` ist eine CAPI Applikation, mit der verschiedene ISDN Datenübertragungsdienste getestet werden können.

Folgende Dienste können eingestellt werden:

- 64 kBits/s senden oder empfangen
- Fax senden oder empfangen
- Fax-Polling
- DATEG-MSV2 Betrieb.

`testhsc` kann entweder aktiv eine Verbindung aufbauen und dann Daten senden, oder auf einen Anruf warten und dann Daten empfangen.

Client-Modus :

`testhsc` überträgt eine Datei zu einer Gegenstelle mit der angegebenen Rufnummer. Folgende Optionen sind verfügbar:

```
testhsc -n rufnummer
  [-s serviceindikator]
  [-1 schicht1]
  [-2 schicht2]
  [-3 schicht3]
  [-4 prot]
  [-b blocklänge]
  [-c controller]
  datei
```

Server-Modus:

testhsc wartet auf eingehende Anrufe und legt die empfangenen Daten in einer Datei ab. Bei fehlendem Dateinamen schreibt *testhsc* die empfangenen Daten auf die Standardausgabe.

Folgende Optionen sind verfügbar:

```
testhsc -d
        [-1 schicht1]
        [-2 schicht2]
        [-3 schicht3]
        [-4 proto]
        [datei]
```

Parameter:

- n** *rufnummer*
Rufnummer der Gegenstelle.
- d**
Legt fest, daß *testhsc* im Server-Modus gestartet werden soll.
- s** *serviceindikator*
Serviceindikator bei abgehenden Rufen laut Dokument [ftz1tr3 87].
- 1** *schicht1*
Schicht 1 Protokoll entsprechend Tabelle der B-Protokolle
- 2** *schicht2*
Schicht 2 Protokoll entsprechend Tabelle der B-Protokolle
- 3** *schicht3*
Schicht 3 Protokoll entsprechend Tabelle der B-Protokolle
- 4** *prot*
Legt eines der folgenden Protokolle fest:
 - msv2
 - fax
- b** *blocklänge*
Legt die maximale Länge der übertragenen Datenpakete in Bytes fest. Der maximal zulässige Wert beträgt 2048. Dies ist auch die Standardeinstellung.

-c controller

Legt den für die Datenübertragung zu verwendenden CAPI-Controllernummer fest. Die CAPI-Controllernummern beginnen mit 1. Fehlt dieser Parameter, so wird der Controller 1 ausgewählt.

Exit Codes:

0: o.k., sonst Fehler.

Beispiel zum Senden von Daten:

Die Datei *test.dat* soll an die Rufnummer *12345* geschickt werden:

```
testhsc -n 12345 test.dat
```

Beispiel zum Empfangen von Daten:

Auf der Empfangsseite soll die gesendete Datei als *neu.dat* abgespeichert werden.

```
testhsc -d neu.dat
```

11.2.3 gpf2

Das Programm *gpf2* zeichnet die Transaktionen von und zur ISDN-Protokollsoftware auf. Zum Speichern der Daten wird das GPF-Format (Generic Protocol Trace Format) verwendet, das die folgende Angaben enthält:

- Zeitstempel
- Protokollnamen (BSC, LAP-B, LAP-D)
- Modemgeschwindigkeit (V.23)
- Controllernummer
- Kanalspezifikation
- Richtung
- Nutzdaten

Die entstandene Binärdatei kann durch das Programm *fascii* in lesbaren ASCII Text konvertiert werden, siehe Kapitel 11.2.5, *fascii*. Optional können vorher einzelne Informationen herausgefiltert oder umformatiert werden. Dies geschieht mit dem Programmen *fppp*, siehe Kapitel 11.2.4. Das Programm *gpf2* muß durch die Tastenkombination *^C* oder das Signal 15 beendet werden.

Unterstützte Funktion:

```

gpf2
  [-c controllerliste]
  [-d debugliste]
  [-C kanalliste]
  [[-F anzahl] [-s dateigröße] file]

```

Parameter:**-C** *kanalliste*

Legt die Kanäle fest, für die Trace-Informationen verarbeitet werden sollen. Der Wert 0 wählt den D-Kanal aus, Werte größer 0 die entsprechenden B-Kanäle.

-d *debugliste*

Schaltet MULTIDATA spezifische Debug-Informationen (siehe Anhang B.4) ein.

-F *anzahl*

Legt die maximale Anzahl der zu erzeugenden Binärdateien fest und numeriert diese durch anhängen einer fortlaufenden Nummer an den Dateinamen durch. Sind alle Dateien bis zur Maximalgröße angewachsen, werden sie in zyklischem Wechsel überschrieben. Fehlt dieser Parameter, so wird nur eine Datei angelegt.

-s *dateigröße*

Legt die Maximalgröße jeder Binärdatei in Bytes fest. Fehlt dieser Parameter, so ist die Dateigröße nur durch den verfügbaren Plattenplatz beschränkt.

file

Die Binärdaten werden, anstatt auf die Standardausgabe, in die angegebene Datei geschrieben.

11.2.4 fppp

fppp ist ein GPF-Dekoder für PPP (Point to Point Protokoll). *fppp* liest von der Standardeingabe und schreibt auf die Standardausgabe im GPF-Format.

11.2.5 fascii

fascii wandelt das binäre GPF-Format in ASCII um. Dabei wird von der Standardeingabe gelesen und auf die Standardausgabe geschrieben.

11.2.6 getcfg

Die Konfigurationsdatei */usr/lib/hermes/isdnd.cfg* liegt im *win.ini* Format vor. Das Kommando *getcfg* dient dazu, den Wert eines Konfigurationsparameters aus dieser Datei auf die Standardausgabe auszugeben.

```
getcfg -s <section> -t <tag> [-d <default_val>]
      [-f <file>]
```

Parameter:

-s *section*

Der Name des Abschnitts in dem der Konfigurationsparameter gesucht wird. Der Abschnittsname wird ohne eckige Klammern angegeben.

-t *tag*

Der Name des Konfigurationsparameters, dessen Wert ausgegeben werden soll.

-d *default_val*

Dieser Wert wird ausgegeben, wenn der Konfigurationsparameter nicht gefunden wird. Falls dieser Parameter nicht angegeben ist und der Konfigurationsparameter nicht gefunden wird, dann wird nichts ausgegeben.

-f *file*

Name der Datei, in der der Konfigurationsparameter gesucht wird. Falls dieser Parameter nicht angegeben ist, wird die Datei */usr/lib/hermes/isdnd.cfg* verwendet.

Beispiel:

```
getcfg -s INTERFACES -t et0 -d 192.168.1.1
```

A Konfigurationsbeispiele

A.1 Callback

Die Beispiele zeigen die Konfiguration in der Datei *isdnd.cfg*.

A.1.1 HERMES H1 ruft HERMES H2 mit CLIP

Für H1 wird keine besondere Konfiguration benötigt.

H2 Konfiguration:

```
[H1Peer]
Callback      = 5           ; nach 5 Sek. zurückrufen
```

A.1.2 HERMES H1 ruft HERMES H2 mit PPP/LCP

H1 Konfiguration:

```
[H2Peer]
PPP           = H2PPP

[H2PPP]
LCP           = H2LCP
CHAP         = H2CHAP

[H2LCP]
CallbackMode = 8           ; 8=Outgoing, 4=Incoming
CallbackType = 0           ; User authentication

[H2CHAP]
LocalName    = H1
RemotePassword = P2
```



H2 Konfiguration:

```
[H1Peer]
PPP      = H1PPP

[H1PPP]
LCP      = H1LCP
CHAP     = H1CHAP

[H1LCP]
CallbackMode = 4      ; 8=Outgoing, 4=Incoming

[H1CHAP]
RemoteName  = H1
LocalPassword = P2
```

A.1.3 WinNT ruft HERMES H2 mit CBCP

WinNT Konfiguration:

1. DFÜ-Netzwerk->>Weiteres->Benutzereinstellung->Rückruf->Vielleicht.
Beim Wählen nachfragen, wenn Server dies anbietet.
2. Wählen->Benutzername W1. Kennwort: W2. Kennwort speichern

H2 Konfiguration:

```
[W1Peer]
PPP      = W1PPP

[W1PPP]
LCP      = W1LCP
CHAP     = W1CHAP

[W1LCP]
CallbackMode = 4      ; 8=Outgoing, 4=Incoming

[W1CHAP]
RemoteName  = W1
LocalPassword = W2
```

A.2 Accounting Restricted Dialout

Innerhalb von 24 Stunden sollen nicht mehr als 100 Gebühreneinheiten anfallen, die Anzahl der abgehenden Verbindungen 50 nicht überschreiten und die Summe der Verbindungszeiten 60 Minuten nicht überschreiten.

```
[ISDND]
ARDInterval = 24
ARDCharge   = 100
ARDCount    = 50
ARDDuration = 60
```


B Tabellen

B.1 Tabelle der wichtigsten CIP Werte

Bitmaske	Bitnr.	Beschreibung
2	1	Speech (Sprache)
4	2	Unrestricted Digital Information (64 kBits/s)
8	3	Restricted Digital Information
16	4	3.1 kHz Audio (Rufe aus dem analogen Netz)
32	5	7 kHz Audio
64	6	Video
128	7	Packet Mode
256	8	56 kBits/s Rate Adaption
512	9	Unrestricted Digital Information with tones/announcements

B.2 Tabelle der B-Protokolle

B.2.1 Schicht 1 Protokolle

0	64 kBits/s with HDLC framing
1	64 kBits/s bit-transparent operation with byte framing from the network
2	V.110 asynchronous operation with start/stop byte framing
3	V.110 synchronous operation with HDLC framing
4	T.30 modem for fax group 3
7	Modem with full negotiation (B2 Protocol must be 7)
8	Modem asynchronous operation with start/stop byte framing
9	Modem synchronous operation with HDLC framing
10	Modem halfduplex operation for MSV2
12	V.110 asynchron with ISO 3309 framing

B.2.2 Schicht 2 Protokolle

0	ISO 7776 (X.75 SLP)
1	Transparent
4	T.30 for fax group 3
5	Point-to-Point Protocol (PPP)
6	Transparent (ignoring framing errors of B1 protocol)
7	Modem with full negotiation (e.g. V.42 bis, MNP 5)
8	ISO 7776 (X.75 SLP) modified supporting V.42bis compression
10	DATEG MSV2

B.2.3 Schicht 3 Protokolle

0	Transparent
1	T.90NL with compatibility to T.70NL in accordance with T.90
2	ISO 8208 (X.25 DTE-DTE)
4	T.30 for fax group 3
5	T.30 for fax group3 with extensions
7	Modem
10	DATEG MSV2

B.3 CAPI Fehlermeldungen

CAPI Fehlermeldungen sind in sogenannte "Fehlerklassen" unterteilt. Ein CAPI-Fehlercode besteht aus einem 16 Bit-Wert, wobei die höherwertigen 8 Bit die Fehlerklasse darstellen. CAPI Fehlercodes können bei der Durchführung von CAPI-Operationen (wie z.B. CAPI_REGISTER oder CAPI_RELEASE) entstehen oder in CONFirmation oder INDication Nachrichten enthalten sein.

Fehlercodes, die bei der Ausführung einer CAPI Operation als Rückgabewert erhalten werden oder in einer CONFirmation Nachricht enthalten sind, signalisieren der Anwendung im Normalfall, daß die gewünschte Operation nicht durchgeführt wurde.

Im folgenden werden einige im praktischen Betrieb häufiger auftretende Fehler mit ihren möglichen Ursachen sowie deren Behebung aufgeführt:

Fehlercodes bei CAPI_REGISTER

0x1001	Too many applications Es sind zu viele Anwendungen registriert (Die Implementation der CAPI unterstützt max. n Anwendungen). Beenden Sie eine andere CAPI-Anwendung.
0x1004	Message buffer size too small, must be at least 1024 bytes Die Anwendung hat im Parameter "MessageBufferSize" einen zu kleinen Wert angegeben. Verwenden Sie bei CAPI_REGISTER einen höheren Wert für den Parameter "MessageBufferSize".
0x1009	COMMON-ISDN-API not installed Bei Verwendung der Remote-CAPI: Es kann keine Netzwerkverbindung zur ISDN-Hardware hergestellt werden. Überprüfen sie die Netzwerkverbindung zum Zielsystem mit der ISDN-Hardware (Router) sowie ob dort die erforderlichen Dienste gestartet sind.

Fehlercodes bei CAPI_RELEASE, CAPI_PUT_MESSAGE, CAPI_GET_MESSAGE

0x1104	<p>Queue is empty</p> <p>Es liegen keine Nachrichten vor, dies stellt keinen eigentlichen Fehler dar.</p>
0x1105	<p>Queue overflow: a message was lost. This indicates a configuration error. The only recovery from this error is to do the CAPI_RELEASE operation.</p> <p>Der Nachrichtenpuffer zur Anwendung ist überschrieben worden, zumindest eine Nachricht ist verlorengegangen. Dieser Fall kann eintreten, wenn CAPI Nachrichten zur Anwendung schneller produziert als die Anwendung die Nachrichten abholt.</p> <p>Stellen Sie sicher, dass ihre Anwendung die Nachrichten schneller abholt oder erhöhen Sie den Wert für "MessageBufferSize" beim CAPI_REGISTER.</p>
0x1107	<p>The message could not be accepted because of an internal busy condition</p>
0x1108	<p>OS resource error (e.g. no memory)</p>
0x1109	<p>COMMON-ISDN-API not installed</p> <p>Bei Verwendung der Remote-CAPI: Die Netzwerkverbindung zur ISDN-Hardware ist evtl getrennt worden.</p> <p>Überprüfen sie die Netzwerkverbindung zum Zielsystem mit der ISDN-Hardware (Router) sowie ob die dort erforderlichen Dienste gestartet sind bzw. noch laufen.</p>

Fehlercodes in _CONF Nachrichten

0x2002	<p>Illegal Controller/PLCI/NCCI</p> <p>Die Anwendung adressiert einen ungültigen Controller, PLCI oder NCCI; oder der adressierte Controller befindet sich in einem Ausnahmezustand.</p> <p>Überprüfen Sie den adressierten Controller (z.B. mit "hcmd -v") auf Ausnahmezustände. Liegt ein Ausnahmezustand vor, benachrichtigen Sie den Hersteller.</p>
---------------	---

Fehlercodes in DISCONNECT_B3_IND Nachrichten

0x3301	<p>Protocol error Layer 1 (line interrupted)</p> <p>Die physische Verbindung wurde beendet (z.B. die Gegenstelle hat während einer Datenübertragung einfach aufgelegt).</p>
---------------	--

Fehlercodes in DISCONNECT_IND Nachrichten

0x3301	<p>Protocol error, Layer 1</p> <p>Es kann keine physikalische Verbindung zum ISDN hergestellt werden. Überprüfen Sie, ob das Verbindungskabel zum ISDN korrekt angeschlossen ist. Funktionieren auch andere Geräte am gleichen Anschluss nicht, überprüfen Sie ob Ihr ISDN Anschluss gestört ist.</p>
0x3302	<p>Protocol error, Layer 2</p> <p>Es kann keine Schicht-2 Verbindung zur Vermittlung bzw. TK-Anlage hergestellt werden.</p> <p>Überprüfen Sie, ob die Konfiguration ihres Geräts mit der Konfiguration des Anschlusses übereinstimmt (P-P oder P-MP Konfiguration). Bei P-MP Konfiguration muss der TEI-Wert auf "automatic" konfiguriert sein; bei P-P meist auf "fixed:0".</p>
0x3304	<p>The call was given to another application (see LISTEN_REQ)</p> <p>Der eingehende Ruf wurde von einer anderen Anwendung angenommen.</p> <p>Überprüfen Sie die Konfiguration der anderen Anwendungen, die auf der gleichen ISDN-Hardware arbeiten. Wenn Ihre Anwendung bestimmte Rufe in jedem Fall erhalten soll, müssen die anderen Geräte/Anwendungen so eingestellt werden (MSN und/oder Service), dass sie derartige Rufe nicht anzunehmen versuchen.</p>

0x3481	Unallocated (unassigned) number
0x3483	No route to destination Die angegebene Rufnummer existiert nicht. Evtl. wurde die Amtskennziffer nicht angegeben.
0x3490	normal call clearing normal, unspecified Normaler Verbindungsabbau, dies stellt keinen Fehler dar.
0x349A	Non-selected user clearing Die Anwendung hat versucht den Ruf anzunehmen, der eingehende Ruf wurde jedoch von einem anderen Gerät am gleichen Anschluss angenommen. Überprüfen Sie die Konfiguration der anderen Geräte, die am gleichen ISDN-Anschluss angeschlossen sind. Wenn Ihre Anwendung bestimmte Rufe in jedem Fall erhalten soll, müssen die anderen Geräte/Anwendungen so eingestellt werden (MSN und/oder Service), dass sie derartige Rufe nicht anzunehmen versuchen.
0x349C	Invalid number format Die Anwendung verwendet evtl. nicht zugelassene Zeichen in der übergebenen Rufnummer.
0x34A2	No circuit / channel available Alle ISDN-Kanäle am Anschluss sind belegt. Versuchen Sie einen Verbindungsaufbau zu einem späteren Zeitpunkt erneut.
0x34A6	Network out of order
0x34A9	Temporary failure
0x34AA	Switching equipment congestion Die Vermittlung/TK-Anlage ist gestört. Versuchen Sie einen Verbindungsaufbau zu einem späteren Zeitpunkt erneut. Bleibt der Fehler permanent bestehen, kontaktieren Sie die Störungsstelle bzw. den Support des TK-Anlagenherstellers.
0x34D1	Invalid call reference Dieser Fehler kann auftreten, wenn die Anwendung bei einem eingehenden Ruf nach der Signalisierung längere Zeit (> 4sec.) verstreichen lässt, und dann den Ruf mit CONNECT_RESP annehmen möchte. Überprüfen Sie das Zeitverhalten der Anwendung bei der Rufannahme oder verwenden Sie ALERT_REQ unmittelbar bei Erhalt von CONNECT_IND für Rufe, die Sie annehmen möchten.

B.4 ISDN Debug-Informationen

Folgende Tabelle gibt an, welche Debug-Informationen durch Setzen der Bitmaske aufgezeichnet werden. Um beispielsweise alle LLD Debug-Informationen aufzuzeichnen, sind die Bits 0 bis 3 bzw. die Bitmaske 0x000f zu setzen.

Im Internet-Browser wird die Einstellung durch Setzen der Bitmaske vorgenommen, während die gp2-Anwendung die Einstellung als Bitnummer bzw. Liste von Bitnummern benötigt.

Bitmaske	Bitnr.	Beschreibung
0x80000000	31	Firmware-Fehler
0x40000000	30	Firmware-Warnungen
0x20000000	29	MDL-Instanz
0x10000000	28	FLOW-Instanz
0x08000000	27	BIFAC-Instanz
0x04000000	26	Protokollstack
0x02000000	25	phys. Verbindung
0x01000000	24	logische Verbindung
0x00F00000	20-23	NLS-Instanz
0x000F0000	16-19	Link Access Protocol D-Kanal
0x0000F000	12-15	D-Kanal LLD
0x00000F00	8-11	Layer 3
0x000000F0	4-7	Layer 2
0x0000000F	0-3	LLD

B.5 Steuerung der Log-Ausgaben

0	: EMERG	System is unusable
1	: ALERT	Action must be taken immediately
2	: CRIT	critical condition, internal errors
3	: ERR	nonfatal error conditions
4	: WARN	warnings, packets lost
5	: NOTICE	normal, but significant condition
6	: INFO	informational message (accounting)

C Troubleshooting

C.1 Zugang zur Web-Konfiguration

Falls der Router nicht erreichbar ist, dann überprüfen Sie bitte die Konfiguration Ihres Web-Browsers. Es darf kein Proxyserver eingestellt sein.

C.2 Notbetrieb

Wenn der Router nicht mehr ansprechbar ist, dann gibt es die Möglichkeit, den Router im Notbetrieb zu starten. In folgenden Fällen hilft der Notbetrieb, den Router wieder einsatzbereit zu machen:

- nach der Aktualisierung der Firmware ist der Router nicht mehr ansprechbar
- das Kennwort wurde geändert und ist nicht mehr bekannt
- die IP Adresse des Routers ist nicht mehr bekannt
- nach einer Änderung der Konfiguration ist der Router nicht mehr ansprechbar.

Um den Router im Notbetrieb zu starten, gehen Sie bitte folgendermaßen vor:

1. Schalten Sie den Router aus.
2. Drücken Sie mit einer Büroklammer oder etwas Ähnlichem den Taster, welcher sich hinter dem kleinen Loch auf der Rückseite befindet und halten Sie ihn gedrückt.
3. Schalten Sie den Router ein.
4. **Fünf Sekunden** nach dem Einschalten können Sie den Taster auf der Rückseite loslassen.



Im Notbetrieb verwendet der Router ein Notbetriebsystem und eine Standardkonfiguration. Anders als im Auslieferungszustand ist der Router über die **IP Nummer 192.168.1.1** erreichbar. Im Notbetrieb steht nur ein eingeschränkter Funktionsumfang des Routers zur Verfügung. Er dient nur dazu den Router wieder einsatzbereit zu machen.

Im Notbetrieb kann ein neues Image gebrannt werden.

Im Notbetrieb können Sie folgende Einstellungen ändern:

- das Kennwort
- die IP Adresse
- weitere Konfigurationseinstellungen

Die Einstellungen müssen persistent gespeichert werden (Make configuration persistent), damit sie nach einem Neustart übernommen werden.

C.3 Verbindungsaufbau

Zum Test, ob der Router prinzipiell Verbindungen aufbaut, kann folgendes Vorgehen benutzt werden:

Rufen Sie im Web-Browser die Seite /connect/<peer section> auf, um die Telefonnummern des Peer Abschnitts <section> zu wählen. Der Dialout erfolgt, wie bei jedem anderen Ruf, mit dem CIP-Wert (Compatibility Information Profile) 2 für 64 kBits/s Datenübertragung. Die Verbindung kommt nur zustande, wenn an der gerufenen Nummer ein Gerät hängt, das Rufe mit diesem CIP annimmt. Wenn Sie eine direkte Rückmeldung über das Klingeln eines *normalen* Telefons haben möchten, dann geben Sie einen CIP Wert von 1 ein.

Dies geschieht über den versteckten Parameter CIP im Edit Peers Menü:

```
... edit/PEERS/ ... &CIP=1& ...
```

Man geht folgendermaßen vor: Edit Peers ausfüllen und OK wählen. Der abgeschickte URL erscheint im Adressenfeld des Browsers. Dieses Feld ist editierbar. Tragen Sie dort den CIP Wert 1 ein und schicken den URL (nochmal) ab. Wenn Sie möchten, daß auch eine logische Verbindung mit dem Telefon zustandekommt, dann tragen Sie als Schicht 2 Protokoll den Wert 1 für *Transparent* und als Schicht 2 Protokoll den Wert 0 für *Transparent* ein. Das Schicht 1 Protokoll kann nicht konfiguriert werden und ist fest auf den Wert 0 (64 kBits/s with HDLC framing) eingestellt.

- Anhand der Ausgaben der Befehle *route* und *ifconfig* kann die Konfiguration der IP-Schnittstelle überprüft werden (siehe Kapitel 6.2, Die IP-Schnittstelle).
- In der Datei *ihosts* müssen alle Zeilen mit der gleichen Telefonnummer auch das gleiche Schicht 2 und Schicht 3 Protokoll enthalten.
D.h. eine Telefonnummer, an der sowohl ein Windows 95 Rechner mit PPP erreicht werden kann, als auch ein UNIX Rechner mit X.75, die sich zwar durch die IP Nummer unterscheiden, kann durch *isdnd* nicht unterschieden werden, da die Protokollauswahl nur anhand der Telefonnummer vorgenommen wird.
- In der Datei *ihosts* sollte keine IP-Nummer doppelt vorkommen, damit die Zuordnung eindeutig wird.
- In der Datei *ihosts* darf kein Eintrag für die eigene IP-Adresse enthalten sein.

D Begriffe und Abkürzungen

<i>100Base-TX</i>	Bezeichnung für ein 100 MBit/s Twisted-Pair-Verkabelung Netzwerk
<i>10Base-T</i>	Bezeichnung für ein 10 Mbit/s Twisted-Pair-Verkabelung Netzwerk
<i>Accounting</i>	Gebührenerfassung wie Gebührevolumen und Verbindungsdaten
<i>ADSL</i>	Asymmetric digital subscriber line
<i>ARD</i>	Accounting Restricted Dialout; durch Regeln bestimmtes Anwahlverfahren
<i>ARP</i>	Adress Resolution Protocol
<i>ARPA</i>	Advanced Research Projects Agency
<i>BOD</i>	Bandwidth On Demand; automatische Kanalbündelung
<i>CAPI</i>	COMMON-ISDN-API
<i>CAPI20.DLL</i>	Dynamic Link Library für Zugriffe von Windows 3.x Applikationen (16-Bit)
<i>CAPI2032.DLL</i>	Dynamic Link Library für Zugriffe von Windows 9x bzw. Windows NT Applikationen (32-Bit)
<i>CBCP</i>	Callback Control Protocol (MS Callback); Protokoll zum Rückrufmanagement
<i>CIDR</i>	Classless Interdomain Routing; WAN-Routing unabhängig von Class A-, B- oder C-Netzen

- CIP Mask* Selektionsmaske für verschiedene Dienste bei eingehenden Rufen
- CIP Wert* Signalisierter Dienst bei abgehendem Verbindungsaufbau
- CLIP* Calling Line Identification Presentation
- Controller* (CAPI); Eine über die CAPI-Schnittstelle adressierbare Hardware-Einheit, die Zugang zum ISDN ermöglicht. (1..n)
- DSS-1* Digital Subscriber Signalling System No. one protocol
- dynamisches Routing*
Anpassung des Routings aufgrund Veränderung der Netztopologie
- Fax-Polling* Verfahren zur Umkehr der Transferrichtung bei FAX-Verbindung
- Firewall-Mechanismus*
auf definierten Regeln basierende Filter-Methoden für IP-Pakete
- Flußkontrolle*
Steuerung der Datentransfargeschwindigkeit
- ftp* file transfer protocol
- getty* Kontrollprogramm im UNIX-System für eingehende Login-Sessions
- HERMES-IP*
IP-Routingsoftware für verschiedene Plattformen und ISDN-Karten
- HTTP* Hypertext Transfer Protocol
- IAB-Protokolle*
Internet Architecture Board und Adressen
- ICMP* Internet Control Message Protocol
- IMP* Internet Message Processors
- IP* Internet Protocol
- IPCP* Internet Protocol Control Protocol

Nameserver-Dienst

UDP-Dienst zur Auflösung von QDN (Qualified Domain Name) zu IP-Nummern

NAT Network Address Translation

NFS Network File System

PPP Point-to-Point Protocol

PPPoE PPP over Ethernet

RFC Request for Comment

smtp simple mail transfer protocol

TCP Transmission Control Protocol

TCP- bzw. UDP Ports

Nummern zwischen 1 und 65535, die verschiedene Sessions und Dienste unterscheiden

TE Terminal Equipment

TEI Terminal Endpoint Identifier

TTL Time to live

UDI Unrestricted Digital Information, 64kBit/sec

UDP User Datagram Protocol

VCAPI Capi-Schnittstelle, die über das Netz an einen ISDN-Controller weitergereicht wird

VJ compression

VanJacobsen Kompressionsverfahren für den IP-Header im PPP

E Literaturverzeichnis

- capi* 1999 COMMON-ISDN-API, Version 2.0, <http://www.capi.org/>
- ets300* 90 European Telecommunication Standard ETS 300 102-1 Integrated Services Digital Network (ISDN); *User-network interface layer 3; Specifications for basic call control*, European Telecommunication Standards Institute, December 1990.
- ftz1tr3* 87 FTZ-Richtliniensammlung, *Technische Forderungen an digitale Endgeräte mit S₀-Schnittstelle*, FTZ-RichtlS 1 TR 3, Band III, Teil 5, 1 TR 6 D-Kanal Protokoll (Schicht 2 und 3), 1987
- ftz1tr805* 93 FTZ Technische Richtlinie, *Standard-Festverbindungen Digital 64S*, FTZ Technische Richtlinie 1 TR 805, Teil 6b, Juni 1993
- ITU-T G.992.1* ADSL specification
- RFC 1172* The Point-to-Point (PPP) Initial Configuration Options, July 1990
- RFC 1332* The PPP Internet Protocol Control Protocol (IPCP), May 1992
- RFC 1548* The Point-to-Point Protocol (PPP), December 1993
- RFC 1570* PPP LCP Extensions, January 1994
- RFC 1618* PPP over ISDN, May 1994
- RFC 1994* PPP Challenge Handshake Authentication Protocol (CHAP), August 1996

F Garantiebedingungen

Garantieumfang

Die Garantie erstreckt sich auf den ausgelieferte Router HERMES-PRO/X mit all seinen Bauteilen. Sie wird in der Form geleistet, daß Bauteile, die nachweislich trotz sachgemäßer Behandlung und Beachtung des Handbuchs aufgrund von Fabrikations- und Materialfehlern defekt geworden sind, ausgetauscht werden. Die dazu verwendeten Teile sind neu oder neuwertig.

Die MULTIDATA GmbH ist berechtigt, über die Instandsetzung und den Austausch hinaus technische Änderungen (z.B. Firmware-Updates) vorzunehmen, um den Router dem aktuellen Stand der Technik anzupassen. Ein Rechtsanspruch hierauf besteht jedoch nicht.

Die MULTIDATA GmbH übernimmt im Garantiefall die Kosten für Material und Arbeitszeit.

Garantiezeit

Die Garantiezeit beträgt 12 Monate und beginnt mit dem Tag der Lieferung des Routers durch die MULTIDATA GmbH.

Spätere Garantieleistungen bewirken weder eine Verlängerung der Garantiezeit noch setzen sie eine neue Garantiefrist in Lauf. Die Garantiezeit für eingebaute Ersatzteile endet mit der Garantiefrist für den ganzen Router.

Abwicklung

Senden Sie den defekten Router bitte sorgfältig verpackt mit einer ausführlichen Fehlerbeschreibung kostenfrei an die MULTIDATA GmbH. Die Rücksendung des instandgesetzten Routers erfolgt auf Ihre Gefahr und auf Ihre Kosten.

