HERMES-PRO/X+

Handbuch

Version 2.0

Erklärung zum Copyright

AIX® ist ein eingetragenes Warenzeichen der International Business Machines Corporation und Windows NT/2000/XP/7 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

Funktionalität und Datendurchsatz prädestinieren den sehr leistungsfähigen standalone LAN/WAN-Router HERMES-PRO/X+ für den professionellen Einsatz. Er basiert auf der bewährten Routing-Software HERMES-IP und den ISDN Protokollstacks von MULTIDATA.

Der Router besitzt vier Ethernet-Schnittstellen: je eine Schnittstelle für das interne LAN und für die DMZ sowie für zwei WAN-Schnittstellen.

Die zweite WAN-Schnittstelle kann als alternative Internetverbindung konfiguriert werden. Der Router aktiviert automatisch die alternative Internetverbindung, sobald der Internetzugang über die primäre WAN-Schnittstelle ausfällt (Failover, Backup). Durch die Ausfallsicherung ist ein hochverfügbarer Internetzugang für unternehmenskritische Anwendungen realisierbar.

Eine USB-Schnittstelle erweitert die Flexibilität bei Konfiguration, Diagnose und Update.

HERMES-PRO/X+ lässt sich problemlos über einen Webbrowser konfigurieren und installieren.

Seine umfangreiche Firewall-Funktionalität sorgt für ein Plus an Sicherheit im LAN.

HERMES-PRO/X+ ermöglicht die Realisierung von VPNs auf IPSec-Basis über das Internet. IPSec gewährleistet die Authentifizierung der Kommunikationspartner, eine starke Verschlüsselung und die Integrität der Daten.

Da HERMES-PRO/X+ dynamische IP-Nummern in Verbindung mit dynDNS unterstützt, ermöglicht er den flächendeckenden und kostengünstigen Aufbau von VPNs. Besonders hervorzuheben sind die einfache VPN-Konfiguration und die Interoperabiliät mit VPN-Gegenstellen anderer Hersteller.

1 HERMES-PRO

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 NT/2000/XP/7 Clients enthalten. Für den Einsatz unter UNIX bzw. Linux wird eine Klassenbibliothek *(capi2lib.o)* bereitgestellt, welche die Funktionalität eines Remote CAPI Clients realisiert. Somit können CAPI Dienste von Kommunikationsanwendungen im Netz genutzt werden.

1.1 Leistungsmerkmale

Software:

- Redundante WAN-Schnittstelle für erhöhte Ausfallsicherheit
- IP-Routing über ISDN S_0 und Ethernet
- IP-Gateway und PPPoE-Funktionalität
- Unterstützung beider B-Kanäle der S_0-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 2000/XP/Vista/7 und UNIX/Linux
- Kommunikation mit V.23 Modems und Fax Gruppe 3 Geräten
- Vermittlungsprotokoll E-DSS1

Hardware:

- Vier Ethernet-Schnittstellen: 3x10/100/1G und 1x10/100
- ISDN Anschluß über S_0-Schnittstelle
- USB Host Anschluss
- Prozessor: PowerPC mit 666 MHz
- Speicher: 256 MB DDR3 SDRAM, 32 MB NOR-Flash
- vielfältige Statusanzeigen über LEDs
- Steckernetzteil (85VAC-264VAC)
- geringer Leistungsverbrauch (max. 7 Watt), ohne Lüfter
- kompakte Bauform (B*H*T): 105 mm*46 mm*125 mm

1.2 Lieferumfang

Zum Lieferumfang gehören:

- der Router HERMES-PRO/X+ mit Steckernetzteil und dieses Handbuch
- ein 3 m langes gelbes ISDN S_0-Kabel
- ein rotes Ethernetkabel
- ein schwarzes V.24 Kabel

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

2 Installation

2.1 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!

2.2 Anschlußvoraussetzungen

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 Konfigurations-problematik dann entfällt. Ist das NTBA wie bei 2) als Mehrgeräteanschluss konfiguriert, so kann HERMES-PRO/X+ auch wie unter 2) beschrieben angeschlossen werden.

2.3 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 gewährleistet sein!

Gehen Sie beim Anschließen in der folgenden Reihenfolge vor:

1. An der Vorderseite des Gerätes befindet sich eine RJ45-Buchse, welche mit *LAN* beschriftet ist. Schließen Sie diese Buchse mit dem beiliegenden roten Kabel an die Netzwerkkarte Ihres Rechners bzw. an ihren Ethernet-Switch an.
2. Verbinden Sie den WAN1-Port mit Ihrem DSL-Modem oder Ihrem IP-Gateway.
3. Verbinden Sie die ISDN S0-Schnittstelle mit dem mitgelieferten gelben ISDN-Kabel mit ihrer ISDN-Dose.

4. Schliessen sie das Kabel des mitgelieferten Steckernetzteils in die mit *DC* beschriftete Buchse des Routers auf der Rückseite an. Dann können Sie das Steckernetzteil in eine 220 Volt Steckdose stecken.

Sobald das Steckernetzteil den Router mit Strom versorgt, 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 die grünen *LINK*-Leuchtdioden der LAN- und der WAN1-Schnittstelle, sobald das Betriebssystem bereit ist.

2.4 Bedeutung der LED Anzeigen

Auf der Frontplatte von HERMES-PRO/X+ befinden sich zwei Gruppen von LEDs, deren Bedeutung in den folgenden Tabellen erklärt ist:

LED	Farbe	Bedeutung
PWR	Rot	Das Gerät ist mit elektrischer Spannung versorgt (siehe auch 2.5).
ONL	Grün	Eine Internet-Verbindung ist aktiv.
FB	Rot	Die altenative Internet-Verbindung ist aktiv.
VPN	Gelb	Mindestens eine VPN-Verbindung ist aktiv.
US	Rot	Diese LED ist vom Benutzer über das Menü "LED Status" steuerbar.

Tab. 1: Allgemeine LED Anzeigen

Wenn die LEDs *ONL*, *FB*, *VPN* und *US* blinken, dann ist HERMES-PRO/X+ dabei das Betriebssystem zu laden.

LED	Farbe	Bedeutung
S0	Gelb	Aktivierung der phys. 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.

Tab. 2: ISDN LED Anzeigen

2.5 Resettaster

Unterhalb der *PWR*-LED befindet sich ein zurückgesetzter Taster mit den folgenden Funktionen:

1. Durch Betätigen des Tasters für eine kurze Zeit (1 Sekunde) wird ein Reset des Routers ausgelöst.
2. Wird der Taster solange gedrückt bis das Blinken der LEDs *ONL*, *FB*, *VPN* und *US* beendet ist, wird das Notimage gestartet.
3. Wird der Taster länger als 6 Sekunden gedrückt, schaltet sich der Router aus. Die *PWR*-LED blinkt in diesem Fall alle 3 Sekunden für etwa 0,2 s.

Weiterhin blinkt die *PWR*-LED bei Übertemperatur im Rhythmus 0,5 s an und 0,5 s aus. Bei Störungen der Stromversorgung blinkt die LED im Rhythmus 1 s an, 1s aus.

2.6 Erste Schritte

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

Schnittstelle	IP Adresse	Neztmaske
Ethernet	192.168.1.254	255.255.255.0
ISDN tun0	192.168.3.1	
Routerprozeß isdnd	192.168.4.1	

Tab. 3: 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 folgenden Menüpunkt auswählen:

Make configuration persistent

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.

3 Ethernet-Schnittstellen

3.1 Übersicht

Der Router hat vier Ethernetschnittstellen, deren Verwendung aus der folgenden Tabelle hervor geht.

Beschriftung	Intern	Geschwindigkeit	Verwendung
LAN	eth0	10/100/1000MBits	LAN
DMZ	eth1	10/100/1000MBits	DMZ (siehe Kapitel DMZ)
WAN1	eth2	10/100/1000MBits	WAN
WAN2	eth3	10/100MBits	WAN Failover

Tab. 4: Ethernet-Schnittstellen

Jeder Ethernet-Schnittstelle ist eine grüne und eine gelbe LED zugeordnet. Die grüne LED leuchtet, wenn die Verbindung auf der Ethernet-Ebene aktiv ist (Link aktiv), und blinkt, wenn Daten über die Schnittstelle übertragen warden. Die gelbe LED zeigt an, dass die für die jeweilige Schnittstelle höchst mögliche Übertragungsrate zwischen den Link-Partnern ausgehandelt wurde.

4 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 Menory Sticks eingesetzt werden können.

4.1 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\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.

4.2 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
```

5 Routerfunktion

5.1 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 *tun0*
- dem Benutzerprozeß *isdnd*
- dem CAPI-Treiber *capi20*.

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

5.2 Die IP-Schnittstelle

Die Schnittstelle zum TCP/IP Protokoll-Stack bildet der *tun* Treiber, der sich als Netzwerkschnittstelle *tun0* darstellt. Alle IP-Pakete werden transparent zu dem Benutzerprozeß *isdnd* durchgereicht. Das Vorhandensein der Netzwerkschnittstelle zeigt der Befehle:

```
ifconfig tun0
tun0  Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
      inet addr:192.168.2.104  P-t-P:192.168.3.104  Mask:255.255.255.255
      UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1454  Metric:1
      RX packets:0 errors:0 dropped:0 overruns:0 frame:0
      TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:500
      RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
```

5.3 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 *tun0* bekannt gemacht. Die Verbindung wird von *tun* 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.

5.4 Datenübertragung

isdnd empfängt von der *tun*-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 *tun*-Schnittstelle übergeben.

5.5 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 *tun*-Schnittstelle ist gewährleistet, daß sporadische IP-Pakete, wie sie z.B. in einem LAN für Routinginfor-

mationen 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 6).

5.6 Routing

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.

5.7 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.

5.8 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.

5.9 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.

5.10 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).

5.11 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 Angerufenenen 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 **Call**.

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 authent-ication	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

5.12 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.

5.13 Interoperabilität

Die Interoperabilität wurde bisher mit folgenden Fremdprodukten getestet:

- SonicWALL
- BIANCA/BRICK
- Cisco
- ITK-Router
- Windows NT/2000/XP/7

MULTIDATA garantiert jedoch nicht für die einwandfreie Zusammenarbeit mit diesen und anderen Produkten.

6 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.

6.1 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.

6.2 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 iptabels 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.

6.3 Chains für HERMES-PRO

Die Routersoftware unterstützt die Konfiguration von IP-Tables über die Weboberfäche und die Konfigurationsdatei isdnd.cfg. Über die Weboberfläche 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 **`iptabels -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 *tun0*-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 (Konfiguartion), 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 benutzerdefinerten Chains generiert isdnd einen eigenen Namensraum, der immer mit der Zeichenkette isdnd-fw: beginnt (Sonderzeichen, wie z. B. "-" oder ":" werden von iptabels 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.

6.4 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 gwünscht, 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)
```

6.5 Konfigurationsmenüs

6.5.1 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	

6.5.2 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 6.3 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.

6.5.3 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 löschbar. 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		insert before

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 6.7 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 6.7 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.

6.6 Format der Konfigurationsdatei

6.6.1 Abschnitt [IPTABLESSECTIONS]

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

IPTABLESSECTn = ***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.

IPTABLESDESCn = ***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.

6.6.2 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 durchnumeriert.

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***

6.7 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

6.8 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

6.9 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 isdnd-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.

6.10 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"
```

7 Demilitarisierte Zone

Eine Demilitarisierte Zone (DMZ) bezeichnet ein Netzwerk mit besonderen Zugriffsrechten auf die darin befindlichen Rechner.

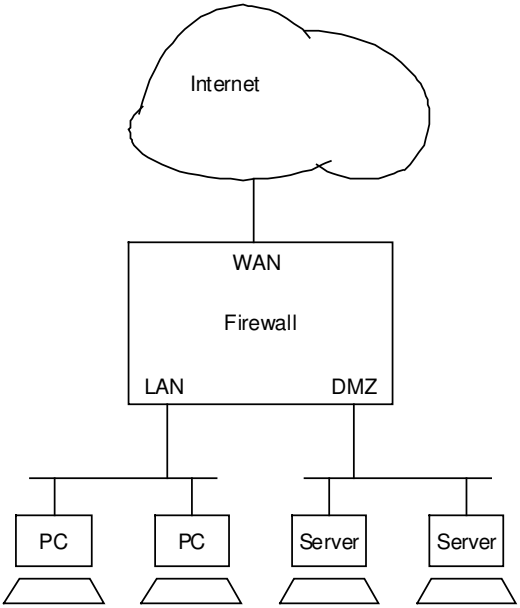

Abb. 7.1: Netzwerkübersicht

Ein typischer Anwendungsfall ist ein HTTP-Server, der vom Internet aus erreichbar sein muss. Dadurch ist er angreifbarer, als die Rechner im LAN und hat somit eine **niedrigere Vertrauensstellung**. Die Firewall zwischen DMZ und LAN verhindert, dass der potenziell korrumpierte HTTP-Server unbeschränkt auf das LAN zugreifen kann. Der Internetzugriff ist für die DMZ-Rechner ohne zusätzliche Einstellungen ebenfalls gesperrt, damit ein gekaperter Rechner z. B. nicht für Distributed Denial of Service Attacken

missbraucht werden kann. Dazu gehört auch, dass Nameserver-Anfragen an den Router von der Firewall verworfen werden.

LAN-Rechner können auf DMZ-Rechner zugreifen. Dafür gelten die gleichen Sicherheitsrichtlinien, wie zwischen LAN-Rechnern und Internet (Siehe *Restrictions for LAN Computers*).

von/nach	LAN	DMZ	Internet
LAN	Ja	Ja	NAT
DMZ	Nein	Ja	Nein
Internet	Nein	Nein	Nein

Tab. 3: Standardberechtigungen

Um einen DMZ-Rechner vom Internet aus erreichbar zu machen, müssen Port Forwarding Regeln angelegt werden. Der Zugriff von DMZ-Rechnern auf das Internet wird über Firewall-Regeln freigeschaltet.

von/nach	LAN	DMZ	Internet
LAN	Ja	Ja	NAT
DMZ	Nein	Ja	Firewall Regel
Internet	Nein	Port Forwarding	Nein

Tab. 4: Berechtigungen für einen Anwendungfall

HERMES-PRO/X+ verfügt über eine Netzwerkschnittstelle, die für den Anschluss des DMZ Netzwerks reserviert ist. DHCP ist an der DMZ-Schnittstelle nicht möglich. Die Rechner in der DMZ müssen manuell eine IP-Adresse zugewiesen bekommen.

7.1 Hinweise zur Konfiguration

Für den Betrieb einer DMZ muss man der DMZ-Schnittstelle eine private IP-Adresse und eine Netzmaske zuweisen. Im Menü *Port Forwarding and DMZ* gibt es ein Untermenü zur Konfiguration der IP-Adresse und der Netzmaske. Das Konfigurationsmenü ist im Abschnitt 12.1.3 Port Forwarding and DMZ beschrieben.

Die Rechner in der DMZ müssen eine IP-Adresse aus dem konfigurierten Adressbereich manuell zugewiesen bekommen. Als Standardgateway und als Nameserver sollte bei den DMZ Rechnern die Adresse der DMZ-Schnittstelle des Routers konfiguriert werden.

Rechner aus dem LAN können nun bereits auf Rechner in der DMZ zugreifen.

Damit die Rechner in der DMZ vom Internet aus erreichbar sind, müssen Port Forwarding Regeln angelegt werden.

Anhand eines Beispiels wird eine mögliche Konfiguration erläutert.

LAN Konfiguration

Netzwerk	192.168.10.0/24
Routerschnittstelle (LAN)	192.168.10.1

DMZ Konfiguration

Netzwerk	192.168.250.0/24
Routerschnittstelle (DMZ)	192.168.250.1
HTTP-Server	192.168.250.64

Wenn der HTTP-Server erreichbar sein soll, dann muss z. B. der Port 80 (http) und der Port 443 (https) freigegeben werden:

Port Forwarding

IP Address	TCP Ports	UDP Ports
192.168.250.64	http, https	

Wenn der HTTP Server für einen reibungslosen Betrieb DNS-Namen auflösen muss, dann muss eine Firewall-Regel angelegt werden, welche die Namensauflösung erlaubt. Der HTTP-Server darf den UDP-Port 53 auf der DMZ-Schnittstelle des Routers erreichen.

IPTABLES

Source IP-Address	Source IP-Mask	Destination IP-Address	Destination IP-Mask	TCP Ports	UDP Ports	Target
192.168.250.64	255.255.255.255	192.168.250.1	255.255.255.255	Any	domain	ACCEPT

Wenn der HTTP-Server einen NTP-Server im Internet für die Aktualisierung der Uhrzeit benötigt, dann muss dieser Port freigeben werden. Da die IP-Adresse des NTP-Servers zum Konfigurationszeitpunkt des Routers evtl. nicht fest steht, kann man die Zieladresse nicht eingeschränken und man muss 0.0.0.0/0.0.0.0 verwenden.

IPTABLES

Source IP-Address	Source IP-Mask	Destination IP-Address	Destination IP-Mask	TCP Ports	UDP Ports	Target
192.168.250.64	255.255.255.255	192.168.250.1	255.255.255.255	Any	domain	ACCEPT
192.168.250.64	255.255.255.255	0.0.0.0	0.0.0.0	ntp	Any	ACCEPT

Weitere Regeln für Berechtigungen der DMZ Rechner kann man nach dem gleichen Schema anfügen.

Wenn im Menü *Restrictions for LAN Computers* Einschränkungen für LAN-Rechner definiert sind, dann muss die vorletzte Regel nach ica@computerlist springen, da dort die dafür zuständigen Regeln abgelegt sind:

IPTABLES

Source IP-Address	Source IP-Mask	Destination IP-Address	Destination IP-Mask	TCP Ports	UDP Ports	Target
192.168.250.64	255.255.255.255	192.168.250.1	255.255.255.255	Any	domain	ACCEPT
192.168.250.64	255.255.255.255	0.0.0.0	0.0.0.0	ntp	Any	ACCEPT
0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	Any	Any	ica@computerlist
0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	Any	Any	RETURN

Die Tabelle muss an die Internetverbindung gebunden werden.

8 IPSec und VPN

Dieses Kapitel beschreibt die Funktionsweise der VPN Implementierung und die VPN Konfiguration.

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 Konfiguartion 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 13.15 Abschnitt [VPNRouten].

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	TCP Port
GnuDIP	3495
DynDNS	80

Tab. 5: 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 Verbindungen mit IPSec-Gegenstellen 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 dem konfigurierten DynDNS Server mit, sobald er mit dem Internet verbunden ist. Dies wiederholt er, falls der eigene Name nicht korrekt aufgelöst werden kann (z. B. wenn der DynDNS Server abstürzt).

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.

Da lediglich die erste Nachricht unverschlüsselt übertragen wird, muss spätestens bei der zweiten Nachricht die Identität der Gegenstelle bekannt sein, damit der richtige Schlüssel verwendet wird. Im Identity Protection Mode stellt der HERMES-Router die Identität der Gegenstelle über die Namensauflösung fest. Im Gegensatz zum Identity Protection Mode kann im Aggressive Mode der Responder dem Initiator einen Konfigurationssatz zuordnen, da im ersten empfangenen Paket seine Identifikation enthalten ist.

Ab der Version 4.x sind mindestens zwei Konfigurationsprofile vordefiniert, welche zur Kompatibilität mit alten Konfigurationen dienen:

Profil	HERMES-3DES	Roadwarrior
Parameter	**Phase 1**	
Verschlüsselung	3DES-CBC	3DES-CBC
Hashverfahren	SHA	SHA
Authentifizierungsmethode	Identity Protection	Aggressive Mode
Authentifizierung	Preshared Key	Preshared Key
Diffie Hellmann Gruppe	1024 Bit MODP (2)	1024 Bit MODP (2)
Lebensdauer	3600 Sekunden	3600 Sekunden
Identifikation	FQDN	FQDN
	Phase 2	
Verschlüsselung	3DES	3DES
Authentifizierung	HMAC_MD5	HMAC_MD5
Kapselung	Tunnel	Tunnel
Lebensdauer	1200 Sekunden	1200 Sekunden

Tab. 6: Kompatibilitätsprofile

Das Konfigurationsprofil **HERMES-3DES** dient der Kompatibilität zu den Versionen 3.x, da die alten Versionen nur dieses eine Profil unterstützen. Dieses Profil entspricht der V3.x Konfigurationsoption **`Phase1Mode = Main`**.

Das Konfigurationsprofil **Roadwarrior** dient der Kompatibilität zur Konfiguration von Gegenstellen, welche nicht am DynDNS teilnehmen, z. B.

Safenet Clients. Dieses Profil entspricht der V3.x Konfigurationsoption **`Phase1Mode = Aggressive`**.

Weitere Konfigurationsprofile dienen erweiterten Einsatzzwecken, wie z. B. der Einsatz von Zertifikaten statt vorinstallierter Schlüssel oder die Verwendung von modernen Verschlüsselungsverfahren (AES). Die Liste der unterstützten Konfigurationsprofile erscheint im Menü `List IKE Configured Peers`.

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. 7: 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 Firewalleinstellungen

Die Firewall ist so eingestellt, dass nur Pakete an den Port 500 (isakmp)n 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
Dynamische IP Adresse	500	esp,icmp	ACCEPT
Dynamische IP Adresse	Any	Any	REJECT

Tab. 8: automatische Firewall-Regeln

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

9 Failover

Dieses Kapitel beschreibt die Anwendungsfälle, die Funktionsweise und die Konfiguration des Failover-Mechanismus.

Der Failover-Mechanismus dient zur Ausfallsicherung der primären Internetverbindung bzw. einer VPN Route. Sobald der Router feststellt, dass die primäre Internetverbindung bzw. die VPN Route ausgefallen ist, baut er eine konfigurierbare, alternative Verbindung auf.

Die Möglichkeit zur Konfiguration mehrerer zusätzlicher Nameserver dient ebenfalls der Ausfallsicherheit.

9.1 Arbeitsweise

Sowohl nach dem Start des Routers als auch nach einem Verbindungsabbau versucht der HERMES-Router eine konfigurierbare Zeitspanne lang die überwachte Verbindung aufzubauen (primäre Internetverbindung oder VPN-Route). Wenn nach Ablauf der Zeitspanne die überwachte Verbindung nicht aufgebaut ist, dann baut er die alternative Verbindung auf und sendet eine E-Mail an den konfigurierten Empfänger.

Ausfall der primären Internetverbindung

Der Router versucht weiterhin die primäre Verbindung aufzubauen, während die alternative Verbindung aktiv ist. Sobald dies erfolgreich ist, baut der Router die alternative Verbindung ab und sendet wiederum eine E-Mail mit der entsprechenden Information.

Ausfall der VPN-Route

Der Router trennt zunächst die primäre Verbindung (falls diese aktiv ist) und baut danach die alternative Internetverbindung auf, gefolgt von dem VPN Verbindungsaufbau. Nach 15 Minuten trennt er die alternative Internetverbindung und reaktiviert die primäre Verbindung.

Alternativ kann der Router eine IP-Adresse mittels **ICMP-Echo-Request (Ping)** überwachen. Die ICMP-Echo-Request Pakete werden alle 2 Sekunden versendet. Wenn 5 Antworten ausbleiben, dann wird die alternative Internetverbindung aktiviert.

9.1.1 Kostenkontroller per E-Mail

Die primäre Internetverbindung ist üblicherweise ein Flatrate-Tarif, bei dem die Kosten klar definiert sind. Die Aktivierung einer alternative Internetverbindung kann jedoch zusätzliche Verbindungskosten verursachen, wenn z. B. eine UMTS-Verbindung mit Volumentarif als Alternative genutzt wird. Damit diese Kosten kontrollierbar werden, kommt eine Benachrichtigung per **E-Mail** zum Einsatz. Sobald der Router eine alternative Verbindung aktiviert, sendet er eine E-Mail an eine konfigurierbare Adresse. Durch organisatorische Vorkehrungen beim Betreiber des Routers muss gewährleistet sein, dass dann Maßnahmen ergriffen werden, welche die Zusatzkosten kontrollieren.

MULTIDATA übernimmt keine Haftung für entstandene Zusatzkosten.

Die automatisch generierte E-Mail enthält im Betreff eine Laufnummer, die Softwareversion und die Seriennummer des Routers.

Beispiel: `#1 4.56HPROX SN634 Testmail`

Ein Administrator bekommt evtl. E-Mails von verschiedenen Routern. Er hat über die eindeutige Seriennummer die Möglichkeit, den Einsatzort des Routers in Erfahrung zu bringen.

9.2 Überwachte Verbindungsarten

Wahlweise kann der Router entweder die primäre Internetverbindung, die Erreichbarkeit einer IP-Adresse oder eine VPN Verbindung überwachen. Die folgenden Kapitel beschreiben die Anwendungsfälle.

9.2.1 Primäre Internetverbindung

Die primäre Internetverbindung kann eine DSL-Verbindung, eine IP-Gateway-Verbindung oder eine ISDN-Verbindung sein und muss "Always On" (**`Timeout = -3`**) konfiguriert sein. Eine IP-Gateway Verbindung ist automatisch "Always On".

In den meisten Fällen wird die primäre Verbindung eine DSL-Verbindung sein, die im Folgenden etwas genauer betrachtet wird.

Bei DSL trennt der Internet Service Provider (ISP) meist nach 24 Stunden Online-Zeit durch eine aktive Benachrichtigung an den Router die Verbindung (Zwangstrennung). Durch die "Always On" Konfiguration baut

der Router die Verbindung nach der Zwangstrennung sofort wieder auf. In der Zeitdauer zwischen der Zwangstrennung und dem erfolgreichen Wiederaufbau ist keine Internetverbindung aktiv.

Die tägliche Zwangstrennung sollte nicht zu einer Aktivierung der alternativen Internetverbindung führen. **Längere** Ausfälle der primären Verbindung müssen jedoch zur Aktivierung der alternativen Verbindung führen. Die Zeitdauer, die als längerer Ausfall gilt, kann im Menü "Failover" konfiguriert werden.

Weitere Gründe, die zu einem kurzfristigen Ausfall der primären Internetverbindung führen, aber nicht zur Aktivierung der alternativen Verbindung führen sollten, sind z. B.:

- Ein Benutzer betätigt im Menü "WAN Connections" den Link "hang up". Durch die "Always On" Konfiguration baut der Router die Verbindung nach wenigen Sekunden wieder auf.
- Ein weiterer Grund für einen kürzeren Ausfall kann direkt nach dem Neustart des Routers auftreten. Das Einwahlmodem des ISPs (DSLAM) reagiert nicht auf den Verbindungsaufbau des Routers, wenn er der Meinung ist, dass bereits eine Verbindung aktiv. Dies kommt meist vor, wenn der HERMES Router im laufenden Betrieb über den Ein-/Ausschalter neu gestartet wird1. Der DSLAM erkennt dann erst nach ca. 2 Minuten, dass die "alte" Verbindung nicht mehr aktiv ist. Erst danach erlaubt der DSLAM wieder einen Verbindungsaufbau. Wenn der Router jedoch über den Menüpunkt "Reboot" neu gestartet wird, dann benachrichtigt er vor dem Herunterfahren den DSLAM. In diesem Fall erlaubt der DSLAM den Verbindungsaufbau sofort, da die alte Verbindung vorher getrennt wurde.

Durch folgende Gründe kann es zu einem längeren Ausfall der primären Internetverbindung kommen. Diese Gründe sollten zur Aktivierung der alternativen Verbindung führen.

- Das DSL-Modem ist defekt oder das Verbindungskabel zwischen Router und Modem hat keinen Kontakt oder ist defekt.
- Das DSL-Modem bekommt keine Verbindung zum DSLAM. Dies kann durch einen defekten Splitter, ein beschädigtes Kabel (z. B. durch Tiefbauarbeiten) oder einen defekten DSLAM verursacht werden. Meist ist das durch eine erloschene "Sync" LED am DSL-Modem erkennbar.

[1] Das gleiche Verhalten tritt auch bei einem kurzen Stromausfall ein.

- Durch defekte oder gestörte Hardware beim ISP ist keine Verbindung zum Einwahlknoten (BRAS) des ISP möglich.

Die Funktionsfähigkeit der Verbindung bis zum BRAS stellt der HERMES-Router durch kontinuierliche PPP-Echo-Anforderung an den BRAS fest. Wenn die Antworten des BRAS für ca. 50 Sekunden ausbleiben, dann trennt der HERMES-Router die Verbindung und kann sie bei den genannten Störungen auch nicht wieder aufbauen. Dies ist der klassische Fall für die Aktivierung der alternativen Verbindung.

Eine fehlerhafte Konfiguration kann ebenfalls zu einem permanenten Ausfall des DSL Zugangs führen. Solche Fehler sollten so schnell wie möglich durch einen Administrator behoben werden.

- Die Authentisierung beim ISP kann fehlschlagen. Dies kann viele Ursachen haben, z. B. eine fehlerhafte Konfiguration der Zugangsdaten im HERMES-Router oder der Ausfall einer Komponente beim ISP, die für die Authentisierung benötigt wird (z. B. Radius Server). Eine mehrfache Anmeldung mit den gleichen Zugangsdaten wird vom ISP ebenfalls zurückgewiesen. Dies kann geschehen, wenn z. B. ein anderes Gerät mit den gleichen Zugangsdaten konfiguriert ist.
- Wenn die Internetverbindung nicht als "Always On", sondern mit einem Timeout-Wert größer 0 konfiguriert ist, dann trennt der HERMES-Router die Verbindung, wenn in der konfigurierten Zeitspanne keine Nutzdaten übertragen wurden. Die primäre Verbindung wird erst dann wieder aufgebaut, sobald ein IP-Paket in das Internet versendet werden soll.

9.2.2 Erreichbarkeit einer IP-Adresse

Wenn die primäre Verbindung eine IP-Gateway Verbindung ist[2], dann kann die Verbindung über ICMP-Echo-Request überwacht werden. Dazu muss für die primäre Verbindung (Type=normal) die "Check Alive Address" im Konfigurationsassistenten eingetragen werden. Die "Check Alive Address" ist im Failover Fall nicht erreichbar, da sie weiterhin über die primäre (ausgefallene) Schnittstelle geleitet wird, um zu erkennen, wann die primäre Verbindung wieder funktioniert.

[2] Dies ist in der Regel bei einem Kabelmodem der Fall.

9.2.3 VPN-Route

Bei der Konfiguration der überwachten Verbindungen kann alternativ zur primären Internetverbindung eine VPN-Route ausgewählt werden. Der IPSEC Tunnelendpunkt für die ausgewählte Route muss eine IKE konfigurierte Gegenseite sein, bei welcher "Auto Tunnel Up" (ATU) aktiv ist. Wenn ATU aktiv ist, sollte die Gegenstelle permanent erreichbar sein. Sie ist nur für die kurze Zeitspanne nicht erreichbar, in der eine Zwangstrennung durch den Internet Service Provider geschieht.

Eine VPN-Route ist aktiv, sobald die Phase 2 Aushandlung des IKE-Protokolls erfolgreich abgeschlossen ist. Das Menü "IPSec and VPN" zeigt eine Liste der VPN Routen und deren Zustand an.

Beide Seiten können die Verbindung trennen und dies der Gegenseite mitteilen. Dies geschieht z. B., wenn der HERMES Router die Internetverbindung aktiv abbaut, weil der Benutzer im Menü "WAN Connections" den Link "hang up" betätigt. Die ATU Konfiguration bewirkt, dass der HERMES Router versucht, die VPN-Verbindung sofort wieder aufzubauen.

Die Verbindung wird auch dann getrennt, wenn die Dead Peer Detection (DPD) feststellt, dass die Gegenseite ca. 50 Sekunden lang nicht mehr auf DPD Anfragen antwortet. In diesem Fall kann der Gegenseite der Verbindungsabbau nicht mitgeteilt werden, da sie ja nicht erreichbar ist. Der HERMES Router versucht weiterhin, die VPN-Verbindung sofort wieder aufzubauen.

Zusätzlich überwacht der Router die DynDNS Adresse der Gegenseite. Sobald sich die IP-Adresse ändert, wird die VPN-Verbindung getrennt, da der Internet Service Provider der Gegenseite eine neue IP-Adresse zugewiesen hat. ATU versucht die Verbindung sofort wieder aufzubauen. Dies kann jedoch wenige Minuten dauern. Dies ist bei der Konfiguration des "Timeout" Parameters zu beachten.

Wenn der Name der Gegenseite nicht aufgelöst werden kann, ist die Gegenstelle vermutlich Offline. In diesem Fall wird die VPN-Verbindung ebenfalls abgebaut. Sie wird erst wieder aufgebaut, wenn sich der Name wieder auflösen lässt.

9.3 Konfiguration

Für die Konfiguration von Failover müssen einige Einstellungen vorgenommen werden.

1. Im Menü Configuration Assistant muss genau eine Internet Verbindung den Typ "normal" zugeordnet sein. Der Parameter Idle muss den Wert "-3" (Always On) haben. Siehe auch: Handbuch für den Konfigurations-assistenen. Eine "Always On" Konfiguration sollte bei bestehenden Installationen der Normalfall sein. Eine IP-Gateway Verbindung ist automatisch "Always On".
2. Mindestens eine weitere Internetverbindung muss konfiguriert werden, die den Typ "failover" hat und auf "Always On" eingestellt ist. Eine IP-Gateway Verbindung ist automatisch "Always On".
3. Im Menü "E-Mail" muss das E-Mail-Konto zur Benachrichtigung der Failover Aktionen eingerichtet werden, damit eine verantwortliche Person eine Kostenkontrolle durchführen kann, sobald eine kostenpflichtige Failover Verbindung aktiviert wird.
4. Im Menü "Failover" muss die überwachte Verbindung, die Zeitdauer bis zur Aktivierung der alternativen Verbindung und die alternative Verbindung konfiguriert werden.
5. Optional kann sowohl die primäre Verbindung als auch die alternative Verbindung mit zusätzlichen Nameservern konfiguriert werden, da dies die Ausfallsicherheit nochmals erhöht.
6. Die Einstellungen müssen persistent gespeichert werden und der Router muss neu gestartet werden.

10 CAPI-Serverfunktion

10.1 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.

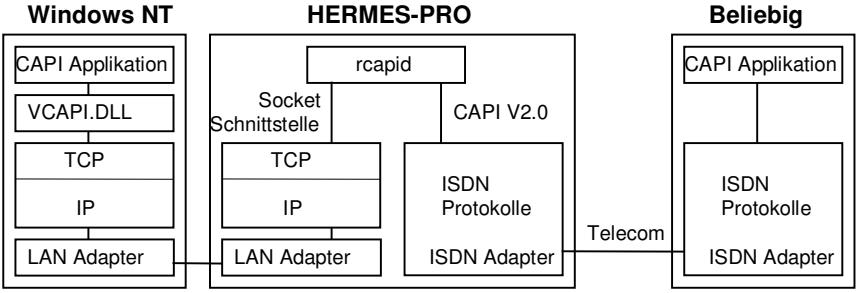

Abb. 10.1: VCAPI Übersicht

10.2 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

10.2.1 Konfiguration von capi2032.dll

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

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

- *HKEY_LOCAL_MACHINE\SOFTWARE\MULTIDATA\VCAPI\Client*
- *VCAPI_SERVER_ADDR*

  die IP Nummer des Servers in Punktschreibweise als Zeichenkette.
- *VCAPI_SERVER_PORT_NO*

  die Portnummer des VCAPI 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.

10.2.2 Multiserver VCAPI

Die capi2032.dll gibt es auch in einer Version, welche mehrere VCAPI-Server unterstützt. Die Konfiguration eines oder mehrerer VCAPI Server geschieht über die Registry. Der Basispfad ist (wie oben):

- *HKEY_LOCAL_MACHINE\SOFTWARE\MULTIDATA\VCAPI\Client*

Jedem Controller, der lokal ansprechbar sein soll, wird ein VCAPI-Server zugeordnet:

- *<localController>\VCAPI_SERVER_CONTROLLER (DWORD)*
- *<localController>\VCAPI_SERVER_ADDR (String)*
- *<localController>\VCAPI_SERVER_PORT_NO (String)*

Wenn ein Server mehrere Controller unterstützt, dann kann für jeden Controller auf dem Server ein RegistryKey eingetragen werden. Die Zahl <localController> muss von 1 aufsteigend sein.

Der Wert **VCAPI_SERVER_CONTROLLER** (Achtung **DWORD**!) gibt die Controllernummer auf dem Server an, welche die capi2032.dll auf die lokale Controllernummer abbildet.

Beispiel:

Es soll ein HERMES-PRO/X+ (S0) mit der IP-Adresse 192.168.1.10 und ein HERMES-PRO/P3 (vier S2M) mit der IP-Adresse 192.168.1.11 konfiguriert werden.

```
....\Client\1\VCAPI_SERVER_CONTROLLER     1
....\Client\1\VCAPI_SERVER_ADDR           192.168.1.10
....\Client\1\VCAPI_SERVER_PORT_NO        7703

....\Client\2\VCAPI_SERVER_CONTROLLER     1
....\Client\2\VCAPI_SERVER_ADDR           192.168.1.11
....\Client\2\VCAPI_SERVER_PORT_NO        7703

....\Client\3\VCAPI_SERVER_CONTROLLER     2
....\Client\3\VCAPI_SERVER_ADDR           192.168.1.11
....\Client\3\VCAPI_SERVER_PORT_NO        7703
```

Dem Client stehen danach drei Controller mit den Nummern 1, 2 und 3 zur Verfügung.

Besonderheiten der Implementierung für mehrere Controller

Die Funktion **CAPI_REGISTER** versucht, eine TCP-Verbindung zu jedem konfigurierten Server aufzubauen. Erst wenn **alle** Verbindungen fehlschlagen, meldet die Funktion den Fehler "CAPI not installed".

Die zurückgegebene Application-ID ist lokal generiert und stimmt nicht mit der Application-ID auf dem Server überein.

Falls für einen Controller kein Server definiert ist, bzw. keine TCP Verbindung zu dem Server besteht, gibt die Funktion **CAPI_PUT_MESSAGE** den Wert **0x2002** "Illegal Controller" zurück. Dieser Wert ist laut CAPI

Spezifikation nicht als Rückgabewert für **CAPI_PUT_MESSAGE** definiert (erlaubt sind nur die Codes **0x11xx**).

Die Funktion **CAPI_INSTALLED** fragt den Server, der die lokale Controllernummer 1 hat.

10.2.3 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.

10.2.4 UNIX

Für verschiedene UNIX Systeme (AIX, Linux) gibt es Multiserver VCAPI Client Implementierungen. Die Schnittstelle zu CAPI Anwendungen dient die vom CAPI Arbeitskreis spezifizierte Shared-Library für Linux. Die Dokumentation liegt in einem eingenständigen Dokument vor: s:\src\mdvclib\mdvclib.doc.

10.3 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.

11 Allgemeines zur Konfiguration

Die Konfiguration von HERMES-PRO/X+ kann über einen Web-Browser und über folgende Konfigurationsdateien erfolgen:

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

Alle Einstellungen über den Web-Browser werden sofort wirksam, falls dies nicht anders angegeben ist. Die Konfigurationsdateien werden nicht automatisch aktualisiert. Im Menü *Configuration Management/Advanced* speichert der Menüpunkt *Save configuration to files* die 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. Damit eine Konfiguration nach dem Neustart des Routers wieder zur Verfügung steht, müssen die Konfigurationsdateien zuerst mit dem Menüpunkt *Configuration Management/Make configuration persistent* im Flash-Speicher abgelegt werden.

12 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/
```

12.1 Interfaces and Routing

In diesem Abschnitt können die Netzwerkschnittstellen und das Routing konfiguriert werden.

12.1.1 Configuration Assistant

Dieses Menü erlaubt die Konfiguration von WAN Gegenstellen.

New Internet (ISDN and DSL/PPPoE)

Peer Name

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

Standardeinstellung: dieser Parameter ist zwingend erforderlich.

Type

Dieses Feld bestimmt, ob dies eine normale oder eine alternative Internetverbindung ist. Eine alternative Internetverbindung steht in der Auswahlliste im Menü Failover zur Verfügung.

Standardeinstellung: **`normal`**.

Telno Call

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

Bei einem Zugang über ein DSL Modem an der WAN1 Schnittstelle müssen Sie pppoe eintragen.

Standardeinstellung: dieser Parameter ist zwingend erforderlich.

Username

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

Wenn die Zeichenkette leer ist, dann erfolgt keine Anmeldung.

Standardeinstellung: leer

Password

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

Wenn die Zeichenkette leer ist, erfolgt keine Anmeldung.

Standardeinstellung: leer

Idle

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

Der Wert -2 bedeutet, dass die Voreinstellung aus dem Menü General Router verwendet wird.

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

Der Wert -3 bedeutet, dass die Verbindung niemals wegen Inaktivität abgebaut wird und immer wieder aufgebaut wird (Always On).

Standardeinstellung: 300

Nameserver Policy

Diese Einstellung bestimmt, welche Nameserver verwendet werden sollen. Bei der Einstellung Provider werden nur die Nameserver des Providers verwendet. Bei der Einstellung Custom werden nur die Nameserver aus dem Feld Nameserver List verwendet. Bei der Einstellung Provider+Custom werden sowohl die Nameserver des Providers als auch die selbst definierten Nameserver verwendet.

Standardeinstellung: Provider

Nameserver List

Hier können Sie eine durch Komma getrennte Liste von Nameservern angeben.

Standardeinstellung: leer

New Internet via IP-Gateway

Mit diesem Menü konfigurieren Sie den Internetzugang über einen externen Router bzw. über ein Kabelmodem.

Peer Name

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

Standardeinstellung: dieser Parameter ist zwingend erforderlich.

Type

Dieses Feld bestimmt, ob dies eine normale oder eine alternative Internetverbindung ist. Eine alternative Internetverbindung steht in der Auswahlliste im Menü Failover zur Verfügung.

Standardeinstellung: **`normal`**.

IP Address

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: leer

Netmask

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: leer

Default Gateway

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: leer

Nameserver Policy

Diese Einstellung bestimmt, welche Nameserver verwendet werden sollen. Bei der Einstellung Provider werden nur die Nameserver des Providers verwendet. Bei der Einstellung Custom werden nur die Nameserver aus dem Feld Nameserver List verwendet. Bei der Einstellung Provider+Custom werden sowohl die Nameserver des Providers als auch die selbst definierten Nameserver verwendet.

Standardeinstellung: Provider

Nameserver List

Hier können Sie eine durch Komma getrennte Liste von Nameservern angeben.

Standardeinstellung: leer

Check Alive Address

Diese IP Adresse wird überwacht, wenn Failover aktiviert ist.

Standardeinstellung: leer

New RAS

In diesem Menü konfigurieren Sie die Einwahl eines Arbeitsplatzes über ISDN.

Peer Name

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

Standardeinstellung: dieser Parameter ist zwingend erforderlich.

Telno Signaled

Anhand der von ISDN signalisierten Rufnummer der Gegenstelle (Calling Party Number) wird bei ankommenden Rufen die Gegenstelle identifiziert und authentisiert. Ist das erste Zeichen ein Stern (*) dann wird die signalisierte Rufnummer von hinten mit der Ziffernfolge verglichen (Postfix Vergleich).

Standardeinstellung: dieser Parameter ist zwingend erforderlich.

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.

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 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*.

Idle

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

Der Wert -2 bedeutet, dass die Voreinstellung aus dem Menü General Router verwendet wird.

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

Die Standardeinstellung beträgt *-2*.

New Router-Router-Connection

In diesem Menü konfigurieren Sie die Verbindung zweier LANs über ISDN.

Peer Name

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

Standardeinstellung: dieser Parameter ist zwingend erforderlich.

Telno Call

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

Wenn kein Dialout durchgeführt werden soll, dann tragen Sie ein Minuszeichen (-) ein.

Standardeinstellung: leer

Telno Signaled

Anhand der von ISDN signalisierten Rufnummer der Gegenstelle (Calling Party Number) wird bei ankommenden Rufen die Gegenstelle identifiziert und authentisiert. Ist das erste Zeichen ein Stern (*) dann wird die signalisierte Rufnummer von hinten mit der Ziffernfolge verglichen (Postfix Vergleich).

Standardeinstellung: dieser Parameter ist zwingend erforderlich.

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.

Password

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

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

IP Address

Die Netzweradresse des entfernten LANs in Punktschreibweise

Standardeinstellung: dieser Parameter ist zwingend erforderlich.

Netmask

Netzmaske des entfernten LANs in Punktschreibweise.

Die Standardeinstellung beträgt *255.255.255.255*.

Idle

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

Der Wert -3 bedeutet, dass die Verbindung niemals wegen Inaktivität abgebaut wird und immer wieder aufgebaut wird (Always On).

Der Wert -2 bedeutet, dass die Voreinstellung aus dem Menü General Router verwendet wird.

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

Die Standardeinstellung beträgt *-2*.

12.1.2 IP Interfaces

Dieses Menü erlaubt die Zuordnung von IP-Nummern und -Masken zu IP-Schnittstellen. Beachten Sie für die Ethernet-Schnittstellen auch das Kapitel 3 Ethernet-Schnittstellen.

Ethernet IP	Ethernet Mask	ISDN Interface	ISDN Router	VLAN for DSL	VLAN ID	
192.168.1.1	255.255.255.0	192.168.3.1	192.168.4.1	No	0	edit

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

VLAN for DSL

Wenn für die DSL Verbindung eine VLAN ID benötigt wird (z. B. bei manchen VDSL Anschlüssen), dann muss der Parameter den Wert Yes enthalten.

Standardeinstellung: No

VLAN ID

Wenn für die DSL Verbindung eine VLAN ID benötigt wird (z. B. bei manchen VDSL Anschlüssen), dann muss dieser Parameter den Zahlwert der VLAN ID enthalten (z. B. 7). Tragen Sie eine Zahl zwischen 0 und 255 ein.

Standardeinstellung: 0

12.1.3 Port Forwarding and DMZ

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.

Eine DMZ (Demilitarisierte Zone) wird eingesetzt, wenn dem Server eine niedrigere Vertrauensstellung ausgesprochen wird und er keinen oder nur eingeschränkten Zugriff auf das private Netz haben soll. Siehe auch Kapitel 7 Demilitarisierte Zone.

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

Port Forwarding

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 6.7 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 6.7 Portdefinition).

Dieser Parameter ist zwingend erforderlich.

Description

Die Beschreibung dient lediglich Dokumentationszwecken.

DMZ

Active	IP Address	Netmask	
Yes	192.168.250.1	255.255.255.0	edit

Active

Dieser Parameter aktiviert die DMZ, wenn der Wert auf **Yes** steht

Die Standardeinstellung beträgt **No**

IP Address

Die IP-Adresse der DMZ Schnittstelle. Diese IP-Adresse muss bei Rechnern in der DMZ als Standardgateway und als Nameserver eingetragen werden.

Standardeinstellung: Dieser Parameter ist zwingend erforderlich.

Netmask

Die Netzmaske für die DMZ.

Standardeinstellung: Dieser Parameter ist zwingend erforderlich.

12.1.4 IPSec and VPN

Dieses Kapitel beschreibt die Konfiguration von VPN Verbindungen. Die Anwendungsfälle und die Funktionsweise beschreibt das Kapitel 8 IPSec und VPN. Der Menüpunkt IPSec and VPN zeigt eine Liste mit Untermenüs und die Tabelle der konfigurierten VPN-Verbindungen an. Die Untermenüs erlauben das Anlegen und Ändern von VPN-Gegenstellen und der VPN-Routing-Tabelle.

IPSec and VPN

- Manual Keyed Peers
- IKE Configured Peers
- VPN Routing Table

Status: Online

Peername	Mode	IP	VPN Routes		
peer1.dyn.domain.de	IKE	84.167.146.19	10.12.123.0	255.255.255.0	active
hub.dyn.domain.de	IKE	188.111.23.12	10.1.0.0	255.255.0.0	active
			10.13.56.0	255.255.255.0	active
peer2.dyn.domain.de	IKE	Offline	192.168.1.0	255.255.255.0	dormant

Die Zeile **Status** zeigt an, ob der Router mit dem Internet verbunden ist ("Online") oder nicht ("Offline").

Die Spalte **Peername** zeigt den konfigurierten FQDN (Full Qualified Domain Name) der Gegenstelle an.

Die Spalte **Mode** zeigt an, ob die IPSec-Parameter für diese Gegenstelle manuell konfiguriert sind ("Manual") oder mittels IKE ausgehandelt werden ("IKE").

Die Spalte **IP** zeigt die aktuelle IP-Adresse der Gegenstelle an. Die IP-Adresse erfragt der Router durch Auflösen des FQDN bei dem aktuellen Nameserver, der sie wiederum vom DynDNS-Server erfragt. Wenn der FQDN nicht auflösbar ist, dann erscheint in dieser Spalte der Status "Offline".

Die Spalte **VPN Routes** zeigt die konfigurierten VPN-Routen und deren Status an. Zu einer Gegenstelle können mehrere Routingeinträge konfiguriert sein. Zu jeder Route wird die Netzwerkadress, die Netzmaske und der Status angezeigt. Wenn eine Verbindung besteht, dann ist der Status "active". Wenn die Verbindung nicht aufgebaut ist, dann ist der Status "dormant".

Untermenü Manual Keyed Peers

In diesem Untermenü können Gegenstellen angelegt werden, deren IPSec Parameter manuell angegeben werden.

Peername	SPI	Shared Secret	Call for Online		
peer3.dyn.domain.de	0x11223344	0x12345678_22345678_32345678_42345678_52345678_62345678	peer3Name	edit	delete

PeerName

Der Name des entfernten Tunnelendpunkts als FQDN (Full Qualified Domain Name).

Wenn die Gegenstelle eine feste IP-Adresse hat und immer 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: **`peer3.dyn.domain.de`**

Standardeinstellung: Dieser Parameter ist zwingend erforderlich.

SPI

Security Parameter Index als hexadezimale Zahl. Der SPI hat einen Wertebereich von 32 Bit. HERMES-PRO verwendet den gleichen SPI sowohl für abgehende als auch für eingehende Pakete. Der SPI muss für beide Tunnelendpunkte gleich sein.

Der SPI muss größer oder gleich 0x200 sein.

Beispiel: **`0x11223344`**

Standardeinstellung: **`0xFFFFFFFF`**

SharedSecret

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. Das Schlüsselmaterial sollte bestimmten Anforderungen genügen, damit die

Verschlüsselung sicher ist. Details zu den Anforderungen finden sich in Spezialliteratur zu Verschlüsselungsverfahren.

Beispiel: `0x12345678_22345678_32345678_42345678_52345678_62345678`

Standardeinstellung: Dieser Parameter ist zwingend erforderlich

CallForOnline

Abschnittsname einer Gegenstelle (WAN Peer). 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.

Beispiel: **`peer3Name`**

Standardeinstellung: leer

Untermenü IKE Configured Peers

In diesem Untermenü können Gegenstellen angelegt werden, deren IPSec Parameter mit Hilfe von IKE (ISAKMP-Protokoll) ausgehandelt werden. Unterhalb der Tabelle der konfigurierten Gegenstellen wird eine Tabelle der vordefinierten IPSec Profile angezeigt.

Peername	Profile	Preshared Key	Route to TE	ATU	Call for Online		
peer1.dyn.domain.de	HERMES-3DES	geh_Heim_nis	direct	No		edit	delete
hub.dyn.domain.de	HERMES-3DES	14d_As	direct	Yes		edit	delete

PeerName

Der Name des entfernten Tunnelendpunkts als FQDN (Full Qualified Domain Name).

Wenn die Gegenstelle eine feste IP-Adresse hat und immer online ist, dann kann der Parameter **`PeerName`** eine IP-Adresse in Punktnotation enthalten.

Beispiel: **`peer1.dyn.domain.de`**

Standardeinstellung: Dieser Parameter ist zwingend erforderlich.

Profile

Der Name eines der vordefinierten Profile mit IKE Parametern. Die Anzahl und die Definition der vorhandenen Profile ist vom Softwarestand abhängig. Das Profil HERMES-3DES ist immer vorhanden. Dieses Profil dient der Kompatibilität zu älteren Versionen.

Beispiel: **`HERMES-3DES`**

Standardeinstellung: Dieser Parameter ist zwingend erforderlich.

Preshared Key

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

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

Beispiel: **`ge_Heim_nis`**

Standardeinstellung: Dieser Parameter ist zwingend erforderlich.

Route to TE

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. Mögliche Werte sind **`via VPN`** und **`direct`** .

Beispiel: **`via VPN`**

Standardeinstellung: **`direct`**

ATU

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: **`Yes`**

Standardeinstellung: **`No`**

CallForOnline

Abschnittsname einer Gegenstelle (WAN Peer). 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.

Beispiel: **`peer3Name`**

Standardeinstellung: leer

Untermenü VPN Routing Table

Dieses Untermenü enthält Routing-Informationen für virtuelle private Netze. Bei einfachen Konfigurationen wird es für jeden IPSec-Gegenstelle genau eine VPN-Route 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).

Peer LAN IP	Netmask	IPSec Tunnel Endpoint	Local Virtual Network Address		
10.12.123.0	255.255.255.0	peer1.dyn.domain.de		edit	delete
10.1.0.0	255.255.0.0	hub.dyn.domain.de		edit	delete
10.13.56.0	255.255.255.0	hub.dyn.domain.de		edit	delete
192.168.1.0	255.255.255.0	peer2.dyn.domain.de	192.168.2.0	edit	delete

Peer LAN IP

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.

Beispiel: **`10.12.123.0`**

Standardeinstellung: Dieser Parameter ist zwingend erforderlich.

Netmask

Netzwerkmaske des entfernten Netzwerks in Punktnotation.

Beispiel: **255.255.255.0**

Standardeinstellung: **255.255.255.0**

IPSec Tunnel Endpoint

Eine der konfigurierten IPSec Gegenstellen. Diese IPSec Gegenstelle wird als Ziel dieses Routing Eintrags verwendet.

Falls der Wert leer ist, dann hat diese Tabellenzeile keine Auswirkungen.

Beispiel: **peer1.dyn.domain.de**

Standardeinstellung: leer

Local Virtual Network Address

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 diese eindeutige Netzwerkadresse 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 hier 0 sein. Wenn der Parameter leer ist, dann wird keine Netzwerkadressumsetzung durchgeführt.

Beispiel: **192.168.2.0**

Standardeinstellung: leer (keine Netzwerkadressumsetzung)

12.1.5 L2TP

Mit L2TP kann man von entfernten Arbeitsstationen auf das LAN zugreifen. Dies geschieht über eine gesicherte Verbindung über das Internet mit Hilfe von IPSec und PPP. Eine Voraussetzung für den Einsatz von L2TP ist, dass die Internet-Adresse des HERMES-Routers entweder statisch ist oder über eine Namensauflösung (z. B: DynDNS) durch die Arbeitsstation abfragbar ist.

Der HERMES Router unterstützt die Konfiguration von genau einer Arbeitsstation. Es ist nicht möglich mehreren Arbeitstationen den Zugriff auf das LAN zu ermöglichen.

Active	Secret	Account	Password	IP Address	
Yes	g_rj7zu+	mobileuser	ba3.pp81	192.168.1.150	edit

Active

Gibt an, ob der Zugriff auf das LAN über L2TP erlaubt werden soll.

Standardeinstellung: **No**

Secret

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

Secret entspricht dem Preshared Key einer IPSec Konfiguration.

Standardeinstellung: Dieser Parameter ist zwingend erforderlich.

Account

Das Benutzerkonto (Benutzername) für die PPP Aushandlung.

Standardeinstellung: Dieser Parameter ist zwingend erforderlich.

Password

Kennwort für die PPP Aushandlung.

Standardeinstellung: Dieser Parameter ist zwingend erforderlich.

AddressForPeer

Die IP-Adresse, die der Gegenstelle bei der PPP Aushandlung zugewiesen wird. Die IP-Adresse muss aus dem Nummernkreis des lokalen Netzes stammen.

Standardeinstellung: Dieser Parameter ist zwingend erforderlich.

12.1.6 Failover

Im Menü "Failover" werden die Einstellungen vorgenommen, um den Failover Mechanismus zu aktivieren.

Observed Connection	Timeout	Alternative	
WAN:dsl-connection	5	ipgateway	edit

Observed Connection

Der Parameter "Observed Connection" bietet als Auswahl die primäre Internetverbindung und alle konfigurierten VPN-Routen. Zur besseren Unterscheidung ist das Kürzel "WAN:" bzw. "VPN:" vorangestellt.

Timeout

Der Parameter "Timeout" hat die Einheit Sekunden. Sobald der Router feststellt, dass die überwachte Verbindung nicht aktiv ist, wartet er die konfigurierte Zeit, bis der die alternative Verbindung aktiviert. Wenn die überwachte Verbindung während der Wartezeit wieder aktiv wird, geschieht nichts.

Alternative

Der Parameter "Alternative" bietet eine Auswahl der Verbindungen, die als "failover"-Verbindung gekennzeichnet sind.

12.2 IP Services

In diesem Abschnitt werden IP Dienste konfiguriert.

12.2.1 Name Service

Dieses Menü behandelt die Auflösung von symbolischen Hostnamen zu IP-Adressen und umgekehrt.

Hosts Database

Hier können Sie die Zuordnung von symbolischen Hostnamen zu IP-Adressen für LAN Rechner treffen. Die Angaben werden in der Datei */etc/hosts* gespeichert. Die Namen dienen dazu, die Konfiguration übersichtlicher zu gestalten. Jeder Konfigurationsparameter, der eine IP-Adresse enthält, kann ebenso mit dem entsprechenden symbolischen Hostnamen spezifiziert werden.

IP Number	Hostname and Aliases		
127.0.0.1	localhost	edit	delete
192.168.1.1	router	edit	delete
192.168.1.2	station1	edit	delete
192.168.1.3	station2	edit	delete

IP-Number

Geben Sie hier die IP-Adresse 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.

DNS Cache

Wenn eine Internetverbindung konfiguriert ist, löst der Router Hostnamen mit Hilfe von Nameservern im Internet auf. Die Ergebnisse kann er in einem lokalen DNS Cache zwischen speichern. Bei einer erneuten Anfrage muss er nicht auf die Antwort eines Internetnameservers warten, sonden kann die Adresse sofort auflösen. Hier können Sie dieses Verhalten einschalten.

Use DNS Cache	
Yes	edit

Use DNS Cache

Gibt an, ob der DNS Cache verwendet werden soll.

Standardeinstellung: **No**

12.2.2 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 (24 Stunden)

Activation and Range

Active	Start Address	End Address	
Yes	192.168.1.128	192.168.1.192	edit

Active

Dieser Parameter aktiviert den DHCP Server, wenn der Wert auf **Yes** steht. Beim Wert **No** ist der DHCP Server deaktiv.

Die Standardeinstellung beträgt **No**

Start Address

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

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 Clinet 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.

12.2.3 Quality of Service

In diesem Menü können Sie die Latenzzeit beim Versenden von IP-Paketen optimieren. Dies ist sinnvoll, wenn Anwendungen zum Einsatz kommen, die kurze Latenzzeiten voraussetzen, wie z. B. Internettelefonie. Über die folgenden Einstellungen können Sie Latenzzeiten vermeiden, die durch Pufferung im DSL Modem entstehen. Dazu müssen Sie dem Router mitteilen, welchen Upstream Durchsatz Ihr Internetzugang hat.

Downstream [kBit/sec]	Upstream [kBit/sec]	
16000	1024	edit

Downstream [kBit/sec]

Tragen sie die Downstream-Rate in kBit pro Sekunde ein. Dieser Wert dient zur Zeit lediglich der Dokumentation und hat keine Auswirkung auf das Verhalten des Routers.

Standardeinstellung: 0

Upstream [kBit/sec]

Tragen sie die Upstream-Rate in kBit pro Sekunde ein. Der Router wird maximal diese Datenrate an das DSL Modem senden. Bei dem Wert 0 findet keine Begrenzung der Datenrate statt.

Standardeinstellung: 0 (QoS ist aus)

12.2.4 DynDNS

Dieses Menü wird benötigt, wenn der Router bei einer Interneteinwahl die IP-Adresse automatisch einem DNS Server mitteilen soll.

Protocol	Hostname	Username	Password	Server	
gnudip	peer7.dyn.domain.de	p7user	******	ns.domain.de	edit

Protocol

Dieses Protokoll wird zur Bekanntgabe der IP-Adresse verwendet. Die unterstützten Protokolle erscheinen in einer Auswahlliste.

Beispiel: **gnudip**

Standardeinstellung: Dieser Parameter ist zwingend erforderlich.

Hostname

Diese Name wird dem DynDNS Server mitgeteilt.

Beispiel: **peer7.dyn.domain.de**

Standardeinstellung: Dieser Parameter ist zwingend erforderlich.

Username

Dieser Parameter wird dem DynDNS Server als Benutzername mitgeteilt.

Beispiel: **p7user**

Standardeinstellung: Dieser Parameter ist zwingend erforderlich.

Password

Dieser Parameter wird dem DynDNS Server als Kennwort mitgeteilt.

Beispiel: **ph12_7M**

Standardeinstellung: Dieser Parameter ist zwingend erforderlich.

Server

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

Beispiel: **ns.domain.de**

Standardeinstellung: Dieser Parameter ist zwingend erforderlich.

12.2.5 IP TV

In diesem Menü können Sie die Einstellungen vornehmen, die für das Telekom Produkt *Home Entertain* (IP TV) benötigt werden.

Active	Profile	VLAN ID	
Yes	Telekom (DHCP)	8	edit

Active

Dieser Parameter aktiviert die Unterstützung von IP TV. Dieser Parameter wird beim nächsten Neustart aktiv.

Die Standardeinstellung beträgt **No**

Profile

Unterschiedliche Generationen verwenden verschiedene Methoden, die IP TV Verbindung zu realisieren. Dieser Parameter bestimmt das Profil der Verbindung. Zur Zeit können Sie zwischen *Telekom (DHCP)* und *Telekom Old*.

Die Standardeinstellung beträgt **Telekom (DHCP)**

VLAN ID

Für manche Profile wird eine VLAN ID benötigt. Tragen Sie hier die VLAN ID ein. Dies ist eine Zahl zwischen 0 und 255.

Die Standardeinstellung beträgt **8**

12.3 System

In diesem Abschnitt befinden sich Systemeinstellungen.

12.3.1 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	NTP Server	Hide Passwords	Disable Telnet	
8	9	7705	30	514	0123456	192.168.1.1	de.pool.ntp.org	Yes	Yes	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 angegebenene 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 5.5, 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 eines Zeitservers (daytime Port) im LAN, 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

NTP Server = *IP-Nummer*

IP-Nummer oder symbolischer Name eines NTP Zeitservers (ntp Port) im Internet, von welchem der Router bei jedem Online gehen das aktuelle Datum und die Uhrzeit erfragt und als Systemzeit setzt. Ist dieses Feld leer, wird keine Einstellung des Datums und der Uhrzeit vorgenommen.

Die Standardeinstellung ist leer

Hide Passwords = `[Yes|No]`

Wenn dieser Wert auf Yes steht, dann werden alle Passwort Felder bei der Eingabe und der Anzeige mit Platzhaltern gefüllt. Wenn der Wert auf No steht, dann werden die Passwörter im Klartext angezeigt.

Die Standardeinstellung ist **No**

Disable Telnet = `[Yes|No]`

Wenn dieser Wert auf Yes steht, dann wird der Zugang zum Router über das Telnet Protokoll gesperrt. Das ssh Protokoll steht Ihnen weiterhin zur Verfügung.

Die Standardeinstellung ist **No**

12.3.2 E-Mail

Bei bestimmten Ereignissen[3] versendet der Router automatisch generierte E-Mails. Als Protokoll für den Postausgang verwendet er SMTP. Wenn ein Kennwort konfiguriert ist, dann setzt der Router als Authentisierungsmethode "AUTH PLAIN" ein. Der SMTP Server muss in diesem Fall die "AUTH PLAIN" Authentisierung unterstützen.

Vorgehen: Der Router prüft im Abstand von 30 Sekunden, ob E-Mails im Postausgangsordner vorliegen. Sobald eine E-Mail erfolgreich versendet wurde, wird sie aus dem Postausgangsordner entfernt. Die E-Mails sind nicht persistent abgelegt, d. h. nach einem Neustart des Routers ist der Ordner leer.

Hinweis: Wenn mehrere Empfänger die E-Mails erhalten sollten, dann bietet es sich an, im SMTP-Server einen Mail-Verteiler anzulegen und diesen als Empfängeradresse einzutragen.

Im Menü "E-Mail" werden die benötigten Parameter konfiguriert.

Wenn die Konfiguration gespeichert ist ("Make configuration persistent"), dann kann man über den Link "Queue Testmail" überprüfen, ob die Konfiguration korrekt ist. Wenn nach einigen Minuten keine E-Mail im Posteingang des Empfängers vorliegt, dann sollte man die Konfiguration nochmals überprüfen. In der Datei /var/log/messages stehen evtl. Hinweise, wieso der E-Mail Versand nicht funktioniert hat.

Server	Account	Password	From	To	Custom Info	
smtp.web.de	routerkonto	rp2sd400	apo@web.de	sol@swh.de	XY Apo	edit

Make configuration persistent

Queue Testmail

Server

IP-Adresse oder DNS-Name des SMTP Servers.

Account

Benutzerkonto bei dem SMTP Server.

Password

Kennwort für das Benutzerkonto beim SMTP Server.

[3] Zur Zeit generiert der Router automatische generierte E-Mails im Rahmen der Kostenkontrolle bei der Aktivierung und Deaktivierung von Failover.

From

E-Mail Adresse des Absenders.

To

E-Mail Adresse des Adressaten.

Custom Info

In dieses Feld können Sie einen kurzen Text eingeben, wecher in die E-Mail mit aufgenommen wird.

12.3.3 Scheduler

Sie können bestimmte Aktionen vom Router zu einer gewissen Zeit erledigen lassen. Es bietet sich zum Beispiel bei DSL Anschlüssen mit Zwangstrennung an, die Trennung der Verbindung aktiv zu einem Zeitpunkt durchzuführen, an dem die Internetverbindung für einige Sekunden ausfallen kann ohne den Arbeitsbetrieb zu stören.

Weekday	Hour	Minute	Action		
Every Day	1	10	Hangup Internet	edit	delete

Weekday

Dieser Parameter ist zur Zeit nicht änderbar.

Standardeinstellung: Every Day

Hour

Tragen Sie hier die Stunde ein, in der die Aktion durchgeführt werden soll.

Standardeinstellung: dieser Parameter ist zwingend erforderlich.

Minute

Tragen Sie hier die Minute ein, in der die Aktion durchgeführt werden soll.

Standardeinstellung: dieser Parameter ist zwingend erforderlich.

Action

In der Auswahlliste stehen Ihnen die Aktionen *Connect Internet* und *Hangup Internet* zur Verfügung.

Standardeinstellung: dieser Parameter ist zwingend erforderlich.

12.3.4 Reboot

Wenn Sie **Reboot** auswählen, wird der Router neu gestartet.

12.4 Configuration Management

In diesem Abschnitt können Sie die Konfiguration speichern, laden und Aktualisierungen durchführen.

12.4.1 Make configuration persistent

Wenn Sie **Make configuration persistent** auswählen, wird die Konfiguration persistent gespeichert.

12.4.2 Update

Bei Anwahl dieses Menüpunktes erscheint ein Formular in dem Sie ein Routerimage oder eine gesicherte Konfiguration auf Ihrem Computer auswählen können. Mit der Schaltfläche **Upload and flash** wird die Datei zum Router übertragen und persistent gespeichert. Der Erfolg bzw. Misserfolg jeder Aktion wird dem Web-Browser zurückgemeldet.

12.4.3 Advanced

Im diesem Untermenü stehen Ihnen folgende Aktionen zur Verfügung:

Make configuration persistent (save and flash)

Wenn Sie **Make configuration persistent** auswählen, wird die Konfiguration persistent gespeichert.

Download configuration as uploadable .tar file

Über dieses Menü können Sie die Konfigurationsdateien des Routers auf Ihren Computer sichern. Die gesicherte Konfiguration können Sie im Menü *Update* wieder auf einen HERMES Router übertragen.

Read configuration from files

Wenn Sie die Konfigurationsdateien im Dateisystem des Routers geändert haben, dann können Sie mit diesem Menüpunkt die geänderte Konfiguration in das laufende System übernehmen.

Save configuration to files

Die Konfiguration des laufenden Systems wird in das Dateisystem des Routers gespeichert. Die Konfiguration wird **nicht** persistent im Flash-Speicher des Routers abgelegt.

Write files to Flash ROM

Die Konfigurationsdateien im Dateisystem werden persistent im Flash-Speicher des Routers abgelegt.

12.5 Firewall

12.5.1 IP-Tables (Firewall)

Siehe Kapitel 6 Firewall-Mechanismus.

12.5.2 Restrict outgoing traffic

In diesem Menü können Sie die Richtlinie für den Internetzugriff für die Computer im LAN einstellen. Die Standardrichtlinie betrifft alle Computer, für die Sie keine individuelle Einstellung vornehmen. Sie können zum Beispiel den Internetzugriff für alle Computer verbieten, und für einige ausgewählte Computer erlauben. Sie können auch allen Computern den Zugriff auf das Internet erlauben und einigen ausgewählen Computern den Zugriff verbieten.

Sie können individuell für jeden Computer einstellen, welche Dienste er im Internet verwenden darf. So können Sie z. B. E-Mail erlauben und das Surfen im Web oder Filesharing-Dienste verbieten.

12.6 Debug

12.6.1 General Router

Über diesen Link erreichen Sie das gleiche Menü, wie über **System/General Router**. In diesem Menü können Sie die Einstellung des Debug Parameters vornehmen.

12.6.2 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 14.2.3 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.

12.7 Information

Abschnitt enthält einige Menüs, welche Ihnen Informationen über den aktuellen Routerzustand anzeigen.

12.7.1 WAN Connections

Dieser Menüpunkt 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 die öffentliche IP Adresse des Routers.

Telno

Telefonnummer der Gegenstelle. Bei einem externen Modem am Port WAN1 wird pppoe 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

12.7.2 TCP Connections

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

TCP Connections

Source IP	Dest. IP	Source Port 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)
93.20.7.15	217.237.148.22	5353	53	180

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

12.7.3 Logfile

Mit diesem Menüpunkt wird die Datei isdnd.log dargestellt.

12.7.4 LED Status

Das Menü "LED Status" zeigt den Zustand der LEDs an (an oder aus). Die Beschreibung der LEDs befindet sich im Kapitel 2.4 Bedeutung der LED Anzeigen.

Online	Failover	VPN	User	
				edit

Mit edit kann man den Zustand der User-LED bestimmen (an oder aus). Der Zustand der User-LED kann nicht persistent gespeichert werden; nach einem Neustart ist die LED immer aus.

12.8 Advanced

12.8.1 WAN Peers

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	255.255.255.2f55	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 1 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 5.11, Callback. Der Wert *-1* bedeutet keinen Rückruf.

Die Standardeinstellung beträgt *-1*.

IP-Table

Legt die für diese Verbindung geltenden Firewallregeln fest. Siehe auch Kapitel 6 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.

12.8.2 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.

12.8.3 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			No	No	edit	delete
lcpm19	Incoming	Location ID		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 5.11, Callback.

Callback Type

Gibt den LCP Callback Typ an. Siehe Kapitel 5.11, Callback.

Callback ID

Gibt die LCP Callback Identifikation an. Siehe Kapitel 5.11, 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*.

12.8.4 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 compr.	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 IPNummer eingetragen.

Die Standardeinstellung beträgt *isdnd.cfg [INTERFACES] mif* (die IP-Nummer der *tun0*-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*.

12.8.5 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	Authenti-cation	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.

12.9 Extras

In diesem Abschnitt befinden sich zusätzliche Konfigurationsmenüs.

12.9.1 Modules

In diesem Menü können Sie sehen, welche optionalen Zusatzmodule geladen sind. Wenn ein Modul nicht geladen werden konnte, dann sehen Sie hier die entsprechende Fehlermeldung.

Name	Loaded	Diagnostics		
/usr/lib/hermes/libledctrl.so	Yes	OK	edit	delete
/usr/lib/hermes/libicmp.so	Yes	OK	edit	delete
/usr/lib/hermes/libfailover.so	Yes	OK	edit	delete

Zur Zeit lassen sich in diesem Menü keine Einstellungen vornehmen.

13 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“).

13.1 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 angegebenene 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**

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 5.5, 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

NTPServer = *IP-Nummer*

IP-Nummer oder symbolischer Name des NTP Servers.

Standardeinstellung: leer

HidePasswords = Yes | No

Unterdrückung der Passwortanzeige.

Standardeinstellung: No

DisableTelnet = Yes | No

Telnet und ftp verhindern.

Standardeinstellung: No

13.2 Abschnitt [*peer*]

Der Name eines Peer-Abschnitts wird aus dem Abschnitt `[PEERSECTIONS]` referenziert. Von dort verweisen die Schlüssel `PEERSECTn` auf die Peer-Abschnitte.

Beispiel:

```
[PEERSECTIONS]
PEERSECT1 = internet
PEERSECT2 = fernwartung
PEERSECT3 = geschaeftstelle1
```

Folgende Parameter sind für diesen Abschnitt definiert:

`Type = [normal | failover]`

Normale oder alternative Verbindung.

Standardeinstellung: **`normal`**

`PeerIP = `*`IP-Nummer`*

IP-Nummer der Gegenstelle. Siehe auch Kapitel 5.7 Besondere Adressen.

Standardeinstellung: **`0.0.0.0`**

`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 5.7 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

OwnTel = *Telefonnummer*

Die Telefonnummer, die der Nebenstellenanlage bzw. Vermittlungsstelle bei abgehenden ISDN Verbindungen als eigene Telefonnummer (Calling Party Number) signalisiert wird. Dieser Parameter kann leer bleiben, da die eigene Telefonnummer in der Regel von der Nebenstellenanlage bzw. Vermittlungsstelle eingesetzt wird.

Standardeinstellung: leer

CIP = *Wert*

Compatibility Information Profile für abgehende Rufe. Siehe B.1 Tabelle der wichtigsten CIP Werte.

Standardeinstellung: **2** (Unrestricted Digital Information)

L1Prot = *Wert*

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

Standardeinstellung: **0**

L1Params = "Liste von Werten"

B Kanal Schicht 1 Protokollparameter. Siehe CAPI Spezifikation.

Beispiel für V.110 8,n,1: "80 25 08 00 00 00 00 00 00 00 01 00"

Standardeinstellung: leer

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 5.12 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 5.11, 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

CheckAliveAddress = *IP-Adresse*

Die Erreichbarkeit dieser Internetadresse wird für die Failover-Überwachung im Fall einer IPGW Konfiguration überprüft.

Standardeinstellung: leer

NameserverPolicy = Wert

Dieser Wert gibt an, welche Nameserver im Internet für Namensauflösungen gefragt werden:

0: Nameserver des Providers

1: Nameserver aus der Liste des Parameters **NameserverList**

2: Nameserver des Providers und zusätzlich die Nameserver aus der Liste des Parameters **NameserverList**

Standardeinstellung: 0

NameserverList = "Liste von IP-Adressen"

Diese Liste enthält die IP-Adressen von manuell konfigurierten Nameservern. Die IP-Adressen sind durch Kommas getrennt.

Beispiel: **"8.8.8.8,208.67.222.222"**

Standardeinstellung: leer

Besondere Werte für den Parameter CALL

Call = pppoe

Der Router baut eine PPPoE Verbindung über ein externes DSL Modem am **Port WAN1** 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 WAN1** (eth2).

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.

GatwayAddress = *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.

13.3 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 Standard-einstellungen 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

13.4 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 5.11, 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 5.11, Callback.

Standardeinstellung: **0**

CallbackID = *Zeichenkette*

Gibt die LCP Callback Identifikation an. Siehe auch Kapitel 5.11, 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**

13.5 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 *tun0* 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: **y**

13.6 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).

13.7 Abschnitt [Failover]

Observed = "WAN:*Abschnittsname*" oder
"VPN:*Peer IP einer VPN Route*" oder
"ICMP:*IP-Adresse*"

Der Abschnittsname der überwachten primären Internetverbindung mit vorangestelltem "WAN:" oder die IP-Adresse einer konfigurierten VPN Route mit vorangestelltem "VPN:" oder die IP-Adresse eines Rechners, der auf Ping antwortet mit vorangestelltem "ICMP:".

Beispiel: **Observed = "WAN:dsl-connection"**
Observed = "VPN:10.123.5.0"

Standardeinstellung: Wenn dieser Parameter nicht vorhanden ist, wird keine Überwachung durchgeführt.

Timeout = "*Zeitdauer in Sekunden*"

Die Wartezeit zwischen der Erkennung, dass die überwachte Verbindung nicht mehr verfügbar ist und der Aktivierung der alternativen Verbindung.

Beispiel: **Timeout = "3"**

Standardeinstellung: Dieser Parameter ist zwingend erforderlich.

Alternative = "*Abschnittsname*"

Der Abschnittsname einer alternativen Internetverbindung. Die angegebene Verbindung muss mit **Type = "failover"** konfiguriert sein. Wenn Failover deaktiviert ist, darf der Parameter eine leere Zeichenkette enthalten.

Beispiel: **Alternative = "ipgateway"**

Standardeinstellung: Dieser Parameter ist zwingend erforderlich.

13.8 Abschnitt [Mail]

Dieser Abschnitt enthält die Konfiguration für das Versenden von E-Mails. Die Parameter **Server**, **From** und **To** sind zum Versenden von E-Mails zwingend erforderlich. Wenn einer dieser Parameter nicht vorhanden ist, dann versendet der Router keine E-Mails.

Server = "*Adresse des SMTP Servers*"

Die Adresse des SMTP-Servers als symbolischer Name oder in Punktschreibweise.

Beispiele: **Server = "smtp.web.de"**
Server = "217.72.192.157"

Standardeinstellung: Dieser Parameter ist zwingend erforderlich.

Account = "*Kontoname*"

Kontoname für die Anmeldung am SMTP-Server. Der Kontoname ist häufig identisch zur Absenderadresse.

Beispiel: **Account = "routerkonto"**

Standardeinstellung: Wenn dieser Parameter nicht vorhanden ist, wird die Absendeadresse verwendet.

Password = "*Kennwort*"

Das Kennwort zur Authentisierung beim SMTP-Server. Wenn das Kennwort nicht vorhanden ist, dann wird keine Authentisierung durchgeführt. Wenn der Server eine Authentisierung fordert, dann können E-Mails nicht erfolgreich versendet werden.

Beispiel: **Password = "rp2sd400"**

Standardeinstellung: leer.

From = "*Absenderadresse*"

Die Absendeadresse für E-Mails. Die Absendeadresse wird auch als Kontoname verwendet, wenn dieser nicht konfiguriert ist.

Beispiel: **From = "hermes-pro@web.de"**

Standardeinstellung: Dieser Parameter ist zwingend erforderlich.

To = "*Empfängeradresse*"

Die Empfängeradresse für E-Mails. Dies kann auch die Adresse eines Mail-Verteilers sein. Mehrere Empfänger können durch Leerzeichen getrennt eingegeben werden. Bei mehreren Empfängern ist darauf zu achten, dass insgesamt nicht mehr als 80 Zeichen erlaubt sind.

Beispiel: **To = "sysop-list@aposw.de"**

Standardeinstellung: Dieser Parameter ist zwingend erforderlich.

CustomInfo = "*Kurzer Text*"

Dieser Text wird in die E-Mail aufgenommen und kann zur Identifizierung des Routers dienen.

Beispiel: **CustomInfo = "Geschäftsstelle 7"**

Standardeinstellung: Leere Zeichenkette.

13.9 Abschnitt [INTERFACES]

fec0 = *IP-Nummer*

Nummer gibt die IP-Nummer der Ethernetschnittstelle an.

Standardeinstellung **192.168.1.1**

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: **192.168.2.1**

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.

Standardeinstellung: **192.168.3.1**

VLANActive = [Yes | No]

Bestimmt, ob eine VLAN ID beim Internetzugang über ein DSL Modem verwendet werden soll.

Standardeinstellung: **No**

VLANId = Zahl

VLAN ID für den Internetzugang. Wertebereich: 0..255

Standardeinstellung: 0

13.10 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.

13.11 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"
IPAdress    = "192.168.1.64"
```

```
[DHCPMapping1]
MACAddress  = "08:00:46:B1:2A:D3"
IPAdress    = "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 Clinet 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.

13.12 Abschnitt [PortForwarding*n*]

Die Abschittsnamen 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 6.7 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 6.7 Portdefinition).

Dieser Parameter ist zwingend erforderlich.

Description = "*Beschreibung*"

Die Beschreibung dient lediglich Dokumentationszwecken.

13.13 Abschnitt [DMZ]

Active = Yes | No

Dieser Parameter aktiviert die DMZ, wenn der Wert auf **Yes** steht

Die Standardeinstellung beträgt **No**

IPAddress = IP-Adresse

Die IP-Adresse der DMZ Schnittstelle. Diese IP-Adresse muss bei Rechnern in der DMZ als Standardgateway und als Nameserver eingetragen werden.

Standardeinstellung: Bei **Active = Yes** ist dieser Parameter zwingend erforderlich.

NetMask = IP-Adresse

Die Netzmaske für die DMZ.

Standardeinstellung: Bei **Active = Yes** ist dieser Parameter zwingend erforderlich.

13.14 Abschnitt [IPSecn]

Die Abschnitte sind aufsteigend beginnend mit 1 numeriert. 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 [VPNRoute*n*] (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 Parameteraushandlung 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. autentifizierten 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 eine erfolgreiche Authentifizierung das gleiche Kennwort verwenden.

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

Beispiel: **PresharedKey = geh_Heim_nis**

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

Profile = "*Profilname*"

Relevant für: **KeyingMode = IKE**

Bei der Aushandlung der Phase 1 und Phase 2 Parameter verwendet HERMES-PRO dieses Konfigurationsprofil. Welche Profile zur Verfügung stehen, können Sie dem Menü `List IKE Configured Peers` entnehmen. Die Profile **HERMES-3DES** und **Roadwarrior** stehen aus Kompatibilitätsgründen immer zur Verfügung.

Die Definition der Profile befindet sich in der Datei */etc/isakmpd/isakmpd.conf*.

Beispiel: **Profile = "Roadwarrior"**

Standardeinstellung: **"HERMES-3DES"**

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

13.15 Abschnitt [VPNRoute*n*]

Dieser Abschnitt enthält Routing-Informationen für virtuelle private Netze. Bei einfachen Konfigurationen wird es für jeden [IPSec*n*] Abschnitt genau einen [VPNRoute*n*] 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 [IPSec*n*] 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 **`IPSec`*`n`*** Abschnitte eindeutig sein.

Beispiel: **`PeerLANIP = 192.168.10.0`**

Standardeinstellung: Dieser Parameter ist zwingend erforderlich.

`Netmask = `*`Netzwerkmaske`*

Netzwerkmaske 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 **`[IPSec`*`n`*`]`** geben, in welchem der Wert **`PeerName`** mit dem hier angegeben Namen übereinstimmt.

Falls der Wert leer ist oder auf keinen **`[IPSec`*`n`*`]`** Abschnitt verweist, dann hat der gesamte **`[VPNRoute`*`n`*`]`** 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)

13.16 Abschnitt [L2TP]

Dieser Abschnitt wird benötigt, wenn eine Arbeitsstation auf das LAN zugreifen können soll.

Active = [Yes | No]

Dieser Parameter aktiviert L2TP.

Standardeinstellung: **No**

SharedSecret = "*Zeichenkette*"

Gemeinsames Kennwort für die IPSec Aushandlung.

Standardeinstellung: dieser Parameter ist zwingend erforderlich

UserAccount = "*Zeichenkette*"

Benutzername für die PPP Aushandlung.

Standardeinstellung: dieser Parameter ist zwingend erforderlich

UserPassword = "*Zeichenkette*"

Kennwort für die PPP Aushandlung.

Standardeinstellung: dieser Parameter ist zwingend erforderlich

AddressForPeer = IP-Adresse

IP-Adresse, die der Gegenstelle zugewiesen wird.

Standardeinstellung: dieser Parameter ist zwingend erforderlich

13.17 Abschnitt [Scheduler*n*]

Dieser Abschnitt enthält Informationen über geplante Aktionen. Die Abschittsnamen müssen von 1 beginnend, aufsteigend nummeriert sein.

Hour = Zahl

Die Stunde des Tages in der die Aktion durchgeführt wird. Wertebereich: 0..23

Standardeinstellung: dieser Parameter ist zwingend erforderlich

Minute = Zahl

Die Minute in der die Aktion durchgeführt wird. Wertebereich: 0..59

Standardeinstellung: dieser Parameter ist zwingend erforderlich

Action = ["Hangup Internet" | "Connect Internet"]

Die Aktion die durchgeführt wird.

Standardeinstellung: dieser Parameter ist zwingend erforderlich

13.18 Abschnitt [DynDNS]

Dieser Abschnitt wird 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 8.2 DynDNS). Eine Konfigurationsänderung der folgenden Parameter wird aktiv, sobald die Konfiguration gespeichert wird und die nächste Interneteinwahl geschieht.

Hostname = *Voll qualifizierter Internet Domänen Name*

Diese Name wird dem DynDNS Server mitgeteilt.

Beispiel: **Hostname = apo1.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. 5: Unterstützte DynDNS Server* aufgeführt.

Beispiel: **Protocol = gnudip**

Standardeinstellung: **gnudip**

User = *Zeichenkette*

Dieser Parameter wird dem DynDNS Server als Benutzername mitgeteilt.

Beispiel: **User = apo1**

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 abweichtene 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.

13.19 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**

14 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.

14.1 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: Betriebssytemkommandos

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 der vom Routingprozeß benötigten Datei /usr/lib/hermes/isdnd.cfg 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.

14.2 HERMES-spezifische Hilfsprogramme

14.2.1 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 Verwechselungen 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**.

14.2.2 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
```

14.2.3 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 14.2.5, fascii. Optional können vorher einzelne Informationen herausgefiltert oder umformatiert werden. Dies geschieht mit dem Programmen *fppp*, siehe Kapitel 14.2.4. 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.

14.2.4 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.

14.2.5 fascii

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

14.2.6 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 Klammen 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
```

B Tabellen

B.1 Tabelle der wichtigsten CIP Werte

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

Fehlercodes in _CONF Nachrichten

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

Fehlercodes in DISCONNECT_B3_IND Nachrichten

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

Fehlercodes in DISCONNECT_IND Nachrichten

0x3301	**Protocol error, Layer 1** 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.
0x3302	**Protocol error, Layer 2** Es kann keine Schicht-2 Verbindung zur Vermittlung bzw. TK-Anlage hergestellt werden. 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".
0x3304	**The call was given to another application (see LISTEN_REQ)** Der eingehende Ruf wurde von einer anderen Anwendung angenommen. 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.

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 desTK-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 gpf2-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 vor, wie in Kapitel 2.5 Resettaster beschrieben.

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.

D Begriffe und Abkürzungen

100Base-TX
: Bezeichnung für ein 100 MBit/s Twisted-Pair-Verkabelung Netzwerk

10Base-T
: Bezeichnung für ein 10 Mbit/s Twisted-Pair-Verkabelung Netzwerk

Accounting
: Gebührenerfassung wie Gebührenvolumen und Verbindungsdaten

ADSL
: Asymmetric digital subscriber line

ARD
: Accounting Restricted Dialout; durch Regeln bestimmtes Anwahlverfahren

ARP
: Adress Resolution Protocol

ARPA
: Advanced Research Projects Agency

BOD
: Bandwidth On Demand; automatische Kanalbündelung

CAPI
: COMMON-ISDN-API

CAPI20.DLL
: Dynamic Link Library für Zugriffe von Windows 3.x Applikationen (16-Bit)

CAPI2032.DLL
: Dynamic Link Library für Zugriffe von Windows 9x bzw. Windows NT Applikationen (32-Bit)

CBCP
: Callback Control Protocol (MS Callback); Protokoll zum Rückrufmanagement

CIDR
: 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 Datentransfergeschwindigkeit

ftp file transfer protocol

getty Kontollprogramm 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
: Unrestriced 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; Sepecifications for basic call controll*, European Telecommunication Standards Institute, December 1990.

ftz1tr3 87 FTZ-Richtliniensammlung, *Technische Forderungen an digitale Endgeräte mit S_0-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.

F