

# **fli4l – flexible internet router for linux**

## **Version 4.0.0-trunk-rpi-r60784**

Das fli4l-Team  
E-Mail: [team@fli4l.de](mailto:team@fli4l.de)

9. Oktober 2022

# Inhaltsverzeichnis

<b>1. Dokumentation des Basispaketes</b>	<b>10</b>
1.1. Einleitung . . . . .	10
<b>2. Installation und Konfiguration</b>	<b>13</b>
2.1. Entpacken der Archive . . . . .	13
2.2. Konfiguration . . . . .	14
2.2.1. Editieren der Konfigurationsdateien . . . . .	14
2.2.2. Konfiguration über eine spezielle Konfigurationsdatei . . . . .	15
2.2.3. Variablen . . . . .	15
2.3. Installationsvarianten . . . . .	15
2.3.1. Router auf einem USB-Stick . . . . .	16
2.3.2. Router auf einer CD oder Netzwerkboot . . . . .	16
2.3.3. Typ A: Router auf Festplatte – nur eine FAT-Partition . . . . .	16
2.3.4. Typ B: Router auf Festplatte – je eine FAT- und ext3-Partition . . . . .	17
<b>3. Basiskonfiguration</b>	<b>18</b>
3.1. Beispiel-Datei . . . . .	19
3.2. Allgemeine Einstellungen . . . . .	28
3.3. Konsolen-Einstellungen . . . . .	35
3.4. Hilfen zum Einkreisen von Problemen und Fehlern . . . . .	36
3.5. Verwendung einer eigenen /etc/inittab . . . . .	37
3.6. Länderspezifische Tastaturlayouts . . . . .	38
3.7. Ethernet-Netzwerkkarten-Treiber . . . . .	38
3.8. Netzwerk-Konfiguration (IPv4) . . . . .	41
3.9. Netzwerk-Konfiguration (IPv6) . . . . .	43
3.9.1. Einleitung . . . . .	43
3.9.2. Adressformat . . . . .	44
3.9.3. Konfiguration . . . . .	45
3.10. Netzwerkpräfix-Konfiguration . . . . .	46
3.10.1. Netzwerkpräfixe vom Typ “stable” . . . . .	47
3.10.2. Netzwerkpräfixe vom Typ “generated-ula” . . . . .	48
3.11. Zusätzliche Routen (IPv4) . . . . .	48
3.12. Zusätzliche Routen (IPv6) . . . . .	49
3.13. Der Paketfilter (IPv4) . . . . .	49
3.13.1. Aktionen des Paketfilters . . . . .	51
3.13.2. Einschränkungen in den Regeln . . . . .	52
3.13.3. Der Einsatz von Schablonen im Paketfilter . . . . .	55
3.13.4. Die Konfiguration des Paketfilters . . . . .	60
3.13.5. Beispiele . . . . .	66
3.13.6. Standardkonfigurationen . . . . .	69

3.13.7. DMZ – Demilitarisierte Zone	74
3.13.8. Conntrack-Helfer	74
3.14. Der Paketfilter (IPv6)	76
3.15. Domain-Konfiguration	82
3.16. imond-Konfiguration	83
3.17. Circuit-Konfiguration	86
3.17.1. Circuits allgemein	86
3.17.2. Circuit-Zustände	94
3.17.3. Wählmodus (DIALMODE)	95
3.17.4. Circuit-Klassen	97
3.17.5. Das Programm <code>fli4lctrl</code>	97
3.17.6. Das Programm <code>circd</code>	100
3.17.7. Wann ist mein Router online?	101
3.17.8. Sonstige Einstellungen	103
3.18. Spezielle Circuit-Typen im base-Paket	103
3.18.1. Circuits vom Typ “route”	103
<b>4. Pakete</b>	<b>105</b>
4.1. Werkzeuge im Basispaket	105
4.1.1. OPT_SYSLOGD – Protokollieren von Systemmeldungen	105
4.1.2. OPT_KLOGD – Protokollieren von Kernelmeldungen	107
4.1.3. OPT_LOGIP – Protokollieren von WAN-IP-Adressen	107
4.1.4. OPT_Y2K – Datumskorrektur bei nicht Y2K-festen Rechnern	107
4.1.5. OPT_PNP – Installation von isapnp tools	108
4.1.6. OPT_HOTPLUG_PCI – Aktivieren von PCI-Hotplugging	110
4.2. Kernel 5.4	110
4.2.1. Netzwerkkartentreiber	110
4.3. Advanced Networking	113
4.3.1. Broadcast Relay - Weiterleitung von IP Broadcasts	113
4.3.2. Bonding - mehrere Netzwerkkarten zusammenfassen zu einem Link	114
4.3.3. VLAN - 802.1Q Unterstützung	118
4.3.4. Device MTU - Anpassen der MTU	119
4.3.5. BRIDGE - Ethernet Bridging für fli4l	119
4.3.6. Anmerkungen	123
4.3.7. EBTables - EBTables für fli4l	123
4.3.8. SWITCH - Switch-Konfiguration	124
4.3.9. ETHTOOL - Einstellungen für Ethernet-Netzwerkadapter	126
4.3.10. Beispiel	127
4.4. CERT - Zertifikatsverwaltung	128
4.5. CHRONY - Network Time Protocol Server/Client	129
4.5.1. Konfiguration des OPT_CHRONY	129
4.5.2. Support	130
4.5.3. Literatur	130
4.6. DNS_DHCP - Dienste rund um DNS und DHCP	131
4.6.1. Hostnamen	131
4.6.2. DNS-Server	132
4.6.3. DHCP-Server	138

4.6.4.	DHCP-Relay . . . . .	142
4.6.5.	DHCP-Client . . . . .	143
4.6.6.	TFTP-Server . . . . .	147
4.6.7.	YADIFA - Slave DNS Server . . . . .	147
4.7.	DSLMODEM - PPP über internes DSL-Modem . . . . .	148
4.8.	DYNDNS - Dynamische Updates für Domain Name Services . . . . .	150
4.9.	EASYSYCRON - Befehle zeitgesteuert ausführen . . . . .	156
4.9.1.	Konfiguration . . . . .	156
4.9.2.	Beispiele . . . . .	157
4.9.3.	Voraussetzungen . . . . .	157
4.9.4.	Installation . . . . .	157
4.10.	HD - Unterstützung von Festplatten, Flash-Karten, USB-Sticks usw. . . . .	158
4.10.1.	OPT_HDINSTALL - Installation auf Festplatte/CompactFlash . . . . .	158
4.10.2.	OPT_MOUNT - Automatisches Einhängen von Dateisystemen . . . . .	160
4.10.3.	OPT_EXTMOUNT - Manuelles Einhängen von Dateisystemen . . . . .	161
4.10.4.	OPT_AUTOMOUNT - automatisches Einhängen von Datenpartitionen . . . . .	162
4.10.5.	OPT_HDSLEEP - automatisches Abschalten für Festplatten einstellen . . . . .	163
4.10.6.	OPT_RECOVER - Notfalloption . . . . .	164
4.10.7.	OPT_HDDRV - Treiber für Festplattencontroller . . . . .	164
4.11.	HTTPD - Status-Webserver . . . . .	165
4.11.1.	OPT_HTTPD - Mini-Webserver als Statusmonitor . . . . .	165
4.11.2.	Nutzerverwaltung . . . . .	166
4.11.3.	OPT_OAC - Online Access Control . . . . .	167
4.12.	HWSUPP - Unterstützung von Hardware . . . . .	169
4.12.1.	Beschreibung . . . . .	169
4.12.2.	Konfiguration des Paketes HWSUPP . . . . .	170
4.12.3.	Experten-Einstellungen . . . . .	175
4.12.4.	Unterstützung von VPN-Karten . . . . .	175
4.13.	IPv6 - Unterstützung von IPv6-Tunneln durch IPv4-Netzwerke . . . . .	176
4.13.1.	Einleitung . . . . .	176
4.13.2.	Konfiguration . . . . .	176
4.14.	ISDN - Kommunikation über aktive und passive ISDN-Karten . . . . .	179
4.14.1.	Herstellen einer ISDN-Verbindung . . . . .	179
4.14.2.	ISDN-Karte . . . . .	180
4.14.3.	OPT_ISDN_COMP (EXPERIMENTAL) . . . . .	183
4.14.4.	ISDN-Circuits . . . . .	184
4.14.5.	OPT_TELMOND - telmond-Konfiguration . . . . .	192
4.14.6.	OPT_RCAPID - Remote CAPI Dämon . . . . .	195
4.15.	OpenVPN - VPN-Support . . . . .	196
4.15.1.	OpenVPN - Einführendes Beispiel . . . . .	197
4.15.2.	OpenVPN - Konfiguration . . . . .	198
4.15.3.	OpenVPN - Bridgekonfiguration . . . . .	201
4.15.4.	OpenVPN - Tunnelkonfiguration . . . . .	202
4.15.5.	Experteneinstellungen . . . . .	205
4.15.6.	OpenVPN - WebGUI . . . . .	216
4.15.7.	OpenVPN - Zusammenarbeit unterschiedlicher OpenVPN Versionen . . . . .	219
4.15.8.	OpenVPN - Beispiele . . . . .	220

4.15.9. Weiterführende Links zum Thema OpenVPN . . . . .	224
4.16. PCMCIA - PC-Card Unterstützung . . . . .	224
4.16.1. PCMCIA-Treiber . . . . .	224
4.17. PPP - Unterstützung für das Point-to-Point-Protokoll . . . . .	225
4.17.1. Circuits vom Typ "ppp" . . . . .	225
4.17.2. Multilink PPP: PPP-Circuits vom Typ "bundle" . . . . .	235
4.17.3. PPP-Circuits vom Typ "serial" . . . . .	240
4.17.4. PPP-Circuits vom Typ "serial-server" . . . . .	240
4.18. PPPOE - PPP über Ethernet . . . . .	242
4.18.1. Ausgehende PPPoE-Verbindungen . . . . .	242
4.18.2. Eingehende PPPoE-Verbindungen . . . . .	243
4.18.3. Beispiele . . . . .	244
4.19. PROXY - Verschiedene Proxy-Server . . . . .	245
4.20. QoS - Quality of Service . . . . .	245
4.20.1. Konfiguration . . . . .	246
4.20.2. Anwendungsbeispiele . . . . .	254
4.21. SSHD - Secure Shell, Secure Copy . . . . .	261
4.21.1. Installation des Secure-Shell-Dienstes . . . . .	261
4.21.2. Installation des dbclients . . . . .	265
4.21.3. Installation des plink Clients . . . . .	266
4.21.4. Installation des sftp-server . . . . .	266
4.21.5. Literatur . . . . .	266
4.22. TOOLS - Zusätzliche Werkzeuge zum Debugging . . . . .	266
4.22.1. Netzwerk-Tools . . . . .	266
4.22.2. Die Hardware-Erkennung . . . . .	272
4.22.3. Dateien-Tools . . . . .	273
4.22.4. Entwickler-Tools . . . . .	274
4.23. UMTS - Anbindung mittels UMTS an das Internet . . . . .	274
4.23.1. Allgemeine UMTS-Konfiguration . . . . .	275
4.23.2. UMTS-Circuit-Konfiguration . . . . .	276
4.24. USB - Support für USB-Geräte . . . . .	277
4.24.1. Probleme mit USB-Geräten . . . . .	278
4.24.2. Hinweise zur Benutzung . . . . .	278
4.24.3. Mounten von USB-Geräten . . . . .	278
4.25. VPN - Unterstützung virtueller privater Netzwerke . . . . .	279
4.25.1. PPTP-Tunnel . . . . .	279
4.25.2. fastd-Tunnel . . . . .	285
4.26. WLAN - Wireless-LAN Unterstützung . . . . .	286
4.26.1. WLAN-Konfiguration . . . . .	286
4.26.2. Weboberfläche . . . . .	291
4.26.3. Beispiele . . . . .	291
4.26.4. Virtual Accesspoint (VAP)(Experimentell) . . . . .	293
4.26.5. Zeitgesteuertes ein- und ausschalten mit easycron . . . . .	293
4.26.6. Spendenhinweis . . . . .	293
4.27. SRC - Das fl4l-Buildroot . . . . .	293
4.27.1. Eine Übersicht über die Quellen . . . . .	294
4.27.2. Übersetzen eines Programms für den fl4l . . . . .	294

4.27.3. Testen eines übersetzten Programms . . . . .	297
4.27.4. Entwanzen eines übersetzten Programms . . . . .	298
4.27.5. Informationen über das FBR . . . . .	301
4.27.6. Ändern der FBR-Konfiguration . . . . .	302
4.27.7. Aktualisierung des FBRs . . . . .	303
4.27.8. Eigene Programme ins FBR einbinden . . . . .	304
<b>5. Erzeugen der fli4l Archive/Bootmedien</b>	<b>305</b>
5.1. Erzeugen der fli4l Archive/Bootmedien unter Linux bzw. anderen Unix-Derivaten und Mac OS X . . . . .	305
5.1.1. Kommandozeilenoptionen . . . . .	306
5.2. Erzeugen der fli4l Archive/Bootmedien unter Windows . . . . .	308
5.2.1. Kommandozeilenoptionen . . . . .	308
5.2.2. Konfigurationsdialog – Einstellung des Konfigurationsverzeichnis . . . . .	309
5.2.3. Konfigurationsdialog – allgemeine Einstellungen . . . . .	310
5.2.4. Konfigurationsdialog – Einstellungen für Remoteupdate . . . . .	311
5.2.5. Konfigurationsdialog – Einstellungen für HD-pre-install . . . . .	312
5.3. Steuerungsdatei mkfli4l.txt . . . . .	313
<b>6. Anbindung von PCs im LAN</b>	<b>315</b>
6.1. IP-Adresse . . . . .	315
6.2. Rechnername und Domain . . . . .	315
6.2.1. Windows 2000 . . . . .	315
6.2.2. NT 4.0 . . . . .	316
6.2.3. Win95/98 . . . . .	316
6.2.4. Windows XP . . . . .	316
6.2.5. Windows 7 . . . . .	317
6.2.6. Windows 8 . . . . .	317
6.3. Gateway . . . . .	317
6.4. DNS-Server . . . . .	318
6.5. Verschiedenes . . . . .	318
<b>7. Client-/Server-Schnittstelle imon</b>	<b>319</b>
7.1. imon-Server imond . . . . .	319
7.1.1. Least-Cost-Routing – Funktionsweise . . . . .	319
7.1.2. Zur Berechnung der Onlinekosten . . . . .	324
7.2. Windows-Client imonc.exe . . . . .	324
7.2.1. Einleitung . . . . .	324
7.2.2. Startparameter . . . . .	325
7.2.3. Seite Überblick . . . . .	327
7.2.4. Config-Dialog . . . . .	328
7.2.5. Seite Anrufe . . . . .	334
7.2.6. Seite Verbindungen . . . . .	334
7.2.7. Seite Fax . . . . .	335
7.2.8. Seite E-Mail . . . . .	335
7.2.9. Admin . . . . .	336
7.2.10. Seiten Fehler, Syslog und Firewall . . . . .	337

7.2.11. Seite News	337
7.3. Unix/Linux-Client imonc	337
<b>8. Entwickler-Dokumentation</b>	<b>340</b>
8.1. Allgemeine Regeln	340
8.2. Übersetzen von Programmen	341
8.3. Modulkonzept	341
8.3.1. mkfli4l	341
8.3.2. Aufbau	342
8.3.3. Die Konfiguration der Pakete	343
8.3.4. Die Liste der zu kopierenden Dateien	343
8.3.5. Die Prüfung der Konfiguration-Variablen	348
8.3.6. Eigene Definitionen zum Prüfen der Konfigurationsvariablen	350
8.3.7. Erweiterte Prüfungen der Konfiguration	356
8.3.8. Unterstützung verschiedener Kernelversionslinien	372
8.3.9. Dokumentation	372
8.3.10. Dateiformate	374
8.3.11. Entwickler-Dokumentation	374
8.3.12. Client-Programme	374
8.3.13. Quellcode	374
8.3.14. Weitere Dateien	375
8.4. Allgemeine Skript-Erstellung auf fli4l	375
8.4.1. Aufbau	375
8.4.2. Umgang mit Konfigurationsvariablen	376
8.4.3. Persistente Speicherung von Daten	376
8.4.4. Fehlersuche	377
8.4.5. Hinweise	378
8.5. Arbeit mit dem Paketfilter	379
8.5.1. Hinzufügen von eigenen Ketten und Regeln	379
8.5.2. Einordnen in bestehende Regeln	380
8.5.3. Erweiterung der Paketfilter-Tests	381
8.6. CGI-Erstellung für das <i>httpd</i> -Paket	382
8.6.1. Allgemeines zum Webserver	382
8.6.2. Skriptnamen	382
8.6.3. Menü-Einträge	382
8.6.4. Aufbau eines CGI-Skriptes	384
8.6.5. Sonstiges	389
8.6.6. Fehlersuche	389
8.7. Hochfahren, Herunterfahren, Einwählen und Auflegen unter fli4l	390
8.7.1. Bootkonzept	390
8.7.2. Start- und Stopp-Skripte	390
8.7.3. Hilfsfunktionen	393
8.7.4. mdev-Regeln	395
8.7.5. ttyI-Geräte	398
8.7.6. Skripte beim Einwählen und Auflegen	398
8.8. Paket „template“	399
8.9. Aufbau des Boot-Datenträgers	400

8.10. Konfigurationsdateien . . . . .	400
8.10.1. Konfiguration Provider . . . . .	401
8.10.2. Konfiguration DNS . . . . .	401
8.10.3. Hosts-Datei . . . . .	402
8.10.4. imond-Konfiguration . . . . .	402
8.10.5. Die <code>/etc/.profile</code> -Datei . . . . .	403
8.10.6. Skripte in <code>/etc/profile.d/</code> . . . . .	403
8.11. Inkompatibilitäten zwischen 3.x und 4.x . . . . .	403
<b>A. Anhang zum Basispaket</b>	<b>404</b>
A.1. Nullmodemkabel . . . . .	404
A.2. Serielle Konsole . . . . .	404
A.3. Programme . . . . .	405
A.4. Andere i4l-Tools . . . . .	405
A.5. Fehlersuche . . . . .	405
A.6. Literaturhinweise . . . . .	406
A.7. Präfixe . . . . .	407
A.8. Gewähr und Haftung . . . . .	407
A.9. Danke . . . . .	407
A.9.1. Projektgründung . . . . .	407
A.9.2. Entwickler- und Testteam . . . . .	407
A.9.3. Entwickler- und Testteam (nicht mehr aktive) . . . . .	408
A.9.4. Sponsoren . . . . .	409
A.10.Feedback . . . . .	410
<b>B. Anhänge der optionalen Pakete</b>	<b>411</b>
B.1. CHRONY - Benachrichtigung anderer Applikationen über Timewarps . . . . .	411
B.2. DYNDNS . . . . .	411
B.2.1. Hinzufügen von neuen Providern . . . . .	411
B.2.2. Dank . . . . .	413
B.2.3. Lizenz . . . . .	414
B.3. EASYCRON - Crontab in der Boot-Phase ergänzen . . . . .	415
B.4. HD - Fehler im Zusammenhang mit Festplatten/CompactFlashes . . . . .	416
B.5. HTTPD . . . . .	417
B.5.1. Zusätzliche Einstellungen . . . . .	417
B.5.2. Allgemeine Bemerkungen . . . . .	417
B.6. HWSUPP - Geräteabhängige Einstellungen . . . . .	418
B.6.1. Verfügbare LED-Devices . . . . .	418
B.6.2. Verfügbare Button-Devices . . . . .	419
B.6.3. Hinweise zu spezieller Hardware . . . . .	420
B.7. HWSUPP - Konfigurations-Beispiele . . . . .	420
B.7.1. generic-pc . . . . .	420
B.7.2. pcengines-apu . . . . .	421
B.7.3. pcengines-apu mit GPIOs . . . . .	421
B.8. HWSUPP - Blinkfolge . . . . .	422
B.9. HWSUPP - Tasten-Codes . . . . .	422



## Inhaltsverzeichnis

B.10.HWSUPP - Hinweise für Paket-Entwickler . . . . .	425
B.10.1. LED-Erweiterungen . . . . .	425
B.10.2. Button-Erweiterungen . . . . .	427
B.10.3. Button-Aktion . . . . .	427
B.11.ISDN . . . . .	428
B.11.1. Technische Details zu Einwahl und Routing bei ISDN . . . . .	428
B.11.2. Fehlermeldungen des ISDN-Subsystems (englisch, i4l-Dokumentation) . . . . .	429
B.12.UMTS . . . . .	431
B.12.1. Unterstützte Hardware . . . . .	431
B.12.2. Modemschnittstelle nicht aktiviert . . . . .	432
B.12.3. Beispiel . . . . .	432
B.13.Unterschiede Version 4.0.0 und 3.6.2 . . . . .	433
B.14.Unterschiede Version 4.0.0 und 3.10.7 . . . . .	444
B.15.Unterschiede Version 4.0.0 und 3.10.8 . . . . .	446
B.16.Unterschiede Version 4.0.0 und 3.10.9 . . . . .	449
B.17.Unterschiede Version 4.0.0 und 3.10.10 . . . . .	451
B.18.Unterschiede Version 4.0.0 und 3.10.11 . . . . .	453
B.19.Unterschiede Version 4.0.0 und 3.10.12 . . . . .	455
B.20.Unterschiede Version 4.0.0 und 3.10.13 . . . . .	457
B.21.Unterschiede Version 4.0.0 und 3.10.14 . . . . .	458
B.22.Unterschiede Version 4.0.0 und 3.10.15 . . . . .	460
B.23.Unterschiede Version 4.0.0 und 3.10.16 . . . . .	461
B.24.Unterschiede Version 4.0.0 und 3.10.17 . . . . .	462
B.25.Unterschiede Version 4.0.0 und 3.10.18 . . . . .	463
<b>Abbildungsverzeichnis</b>	<b>465</b>
<b>Tabellenverzeichnis</b>	<b>466</b>
<b>Index</b>	<b>468</b>

# 1. Dokumentation des Basispaketes

## 1.1. Einleitung

fli4l ist ein auf Linux basierender ISDN-, DSL-, UMTS- und Ethernet-Router mit geringen Anforderungen an die zugrunde liegende Hardware: Ein USB-Stick als Bootmedium, ein Intel Pentium MMX-Prozessor, 64 MiB RAM sowie (mindestens) eine Ethernet-Netzwerkkarte sind dafür vollkommen ausreichend. Das notwendige Bootmedium kann unter Linux, Mac OS X oder MS Windows erstellt werden. Dabei sind keine Linux-Kenntnisse erforderlich, aber durchaus hilfreich. Grundkenntnisse von Netzwerken, TCP/IP, DNS und Routing sollten jedoch vorhanden sein. Für eigene Erweiterungen/Entwicklungen, welche über die Standardkonfiguration hinausgehen, sind ein lauffähiges Linux-System und Linux-Kenntnisse notwendig.

fli4l unterstützt verschiedene Bootmedien, darunter USB-Sticks, Festplatten, CDs und nicht zuletzt das Booten über das Netzwerk. Ein USB-Stick ist in vielerlei Hinsicht ideal: Heutzutage kann so gut wie jeder PC von einem USB-Stick starten, er ist recht erschwinglich, er hat eine ausreichende Größe, und man kann sowohl unter Linux als auch unter MS Windows auf relativ einfache Weise eine fli4l-Installation darauf ablegen. Auch ist er im Gegensatz zu einer CD beschreibbar und kann somit nichtflüchtige Konfigurationsdaten (wie z.B. DHCP-Leases) speichern.

- Allgemeine Features
  - Erstellen von Bootmedien unter [Linux](#) (Seite 305), [Mac OS X](#) (Seite 305) und [MS Windows](#) (Seite 308)
  - Konfiguration über normale ASCII/UTF-8-Dateien
  - Unterstützung von IP-Masquerading und Portweiterleitung
  - Least-Cost-Routing (LCR): automatische Auswahl des Providers, je nach Uhrzeit
  - Anzeige/Berechnung/Protokollierung von Verbindungszeiten und -kosten
  - MS Windows/Linux-Client imonc mit Schnittstelle zu imond und telmond
  - Upload von aktualisierten Konfigurationsdateien über MS Windows-Client imonc oder via SCP unter Linux
  - Bootmedien nutzen das VFAT-Dateisystem zum dauerhaften Speichern von Dateien
  - Paketfilter: Protokollieren von Zugriffen von außen auf gesperrte Ports
  - Einheitliche Abbildung von WAN-Schnittstellen auf sogenannte Circuits
  - Paralleler Betrieb von ISDN- und DSL/UMTS-Circuits ist möglich
- Router-Basisfunktionalität
  - Linux-Kernel 3.18 oder 3.19
  - Paketfilter und IP-Masquerading

## 1. Dokumentation des Basispaketes

- DNS-Server, um die Anzahl von DNS-Abfragen an externe DNS-Server zu reduzieren
- Netzwerkfähiger imond-Server mit Monitor- und LCR-Steuerfunktionen
- Netzwerkfähiger telmond-Server zur Protokollierung von eingehenden Telefonanrufen
- Ethernet-Unterstützung
  - Aktuelle Netzwerkkartentreiber: Unterstützung von über 140 Kartentypen
- DSL-Unterstützung
  - Roaring Penguin PPPoE-Treiber, mit Dial-on-Demand (abschaltbar)
  - PPTP für DSL-Anbindungen in Österreich und den Niederlanden
- ISDN-Unterstützung
  - Unterstützung von knapp 60 ISDN-Kartentypen
  - Mehrere ISDN-Verbindungsmöglichkeiten: eingehend/ausgehend/Rückruf, „roh“/Punkt-zu-Punkt (ppp)
  - Kanalbündelung: automatische Bandbreitenanpassung oder manuelle Zuschaltung des zweiten Kanals über MS Windows-/Linux-Client
- Optionale Programmpakete
  - DNS-Server
  - DHCP-Server
  - SSH-Server
  - Einfache Online/Offline-Anzeige über LED
  - Serielle Konsole
  - Mini-Webserver für ISDN- und DSL-Monitoring sowie zur Rekonfiguration und/oder Aktualisierung des Routers
  - Zugangserlaubnis für bestimmte konfigurierte Netzwerke von außen
  - Unterstützung für PCMCIA-Karten (heutzutage PC-Cards genannt)
  - Protokollierung von Systemmeldungen
  - Konfiguration von ISAPnP-Karten mit den isapnp-Werkzeugen
  - Zusätzliche Werkzeuge zum Debugging
  - Konfiguration der seriellen Schnittstelle
  - Notfallsystem zur Fernwartung über ISDN
  - Software zur Anzeige konfigurierbarer Informationen auf einem LCD, z.B. von Übertragungsraten, CPU-Auslastung etc.
  - PPP-Server/Router über serielle Schnittstelle
  - ISDN-Modem-Emulator über serielle Schnittstelle

## 1. Dokumentation des Basispaketes

- Druckerserver
  - Synchronisierung der Uhrzeit mit externen Zeit-Servers
  - Ausführen von benutzerdefinierten Kommandos bei eingehenden Telefonanrufen (z.B. um ein Internet-Einwahl durchzuführen)
  - Unterstützung von IP-Aliasing (mehrere IP-Adressen pro Netzwerkschnittstelle)
  - VPN-Unterstützung
  - IPv6-Unterstützung
  - WLAN-Unterstützung: fli4l kann sowohl Zugangsknoten als auch Client sein
  - RRD-Tool zum Überwachen des fli4l
  - und vieles andere mehr...
- Hardwarevoraussetzungen
    - Intel Pentium-Prozessor mit MMX Unterstützung
    - 64 MiB Speicher, besser 128 MiB
    - Ethernet-Netzwerkkarte
    - ISDN: unterstützte ISDN-Karte
    - ein USB-Stick, eine ATA-Festplatte oder eine CF-Karte (die genauso wie eine ATA-Festplatte angesprochen wird); alternativ ist auch der Start von CD möglich
  - Softwarevoraussetzungen

Unter Linux werden folgende Programme vorausgesetzt:

    - GCC und GNU make
    - syslinux
    - mtools (mcopy)

Unter MS Windows werden keine zusätzlichen Werkzeuge benötigt, fli4l bringt alles Notwendige mit.

Zusätzlich gibt es zur Steuerung/Statusanzeige des fli4l-Routers noch den Client imonc. Dieses Programm ist für MS Windows (windows/imonc.exe) und auch für Linux (unix/gtk-imonc) vorhanden.

Und nun ...

Viel Spaß mit fli4l!

Frank Meyer und das fli4l-Team

E-Mail: [team@fli4l.de](mailto:team@fli4l.de)

## 2. Installation und Konfiguration

### 2.1. Entpacken der Archive

Unter Linux:

```
tar xvfz fli4l-4.0.0-trunk-rpi-r60784.tar.gz
```

Funktioniert dies nicht, geht's auch so:

```
gzip -d < fli4l-4.0.0-trunk-rpi-r60784.tar.gz | tar xvf -
```

Wer die aktuelle Version in einem bereits existierenden fli4l-Verzeichnis installiert, sollte anschließend `mkfli4l.sh -c` aufrufen, also:

```
cd fli4l-4.0.0-trunk-rpi-r60784
sh mkfli4l.sh -c
```

Es wird jedoch empfohlen, ein neues Verzeichnis für eine neue Version zu benutzen – die Konfiguration kann durch ein entsprechendes Werkzeug zum Dateivergleich sehr einfach übernommen werden.

Unter MS Windows kann das komprimierte Tar-Archiv zum Beispiel mit WinZip extrahiert werden. Dabei ist jedoch zu beachten, dass die Dateien *mit* Unterverzeichnissen (Einstellung in WinZip überprüfen!) ausgepackt werden. Außerdem ist in *Optionen*  $\Rightarrow$  *Konfiguration* die so genannte „Smart TAR CR conversion“ abzuschalten. Ist diese eingeschaltet, werden einige wichtige Dateien von WinZip falsch extrahiert.

Alternativ ist das OpenSource-Programm 7-Zip (<http://www.7-zip.org/>) sehr zu empfehlen, welches ebenso mächtig wie WinZip ist.

Es werden folgende Dateien im Unterverzeichnis `fli4l-4.0.0-trunk-rpi-r60784/` installiert:

- Dokumentation:
  - `doc/deutsch/*` Deutsche Dokumentation
  - `doc/english/*` Englische Dokumentation
  - `doc/french/*` Französische Dokumentation
- Konfiguration:
  - `config/*.txt` Konfigurationsdateien, diese müssen bearbeitet werden
- Skripte/Prozeduren:
  - `mkfli4l.sh` Boot-Medium oder Dateien erzeugen: Linux/Unix-Version
  - `mkfli4l.bat` Boot-Medium erzeugen: Windows-Version

- Kernel/Boot-Dateien:
  - img/kernel Linux-Kernel
  - img/boot\*.msg Bootscreen Texte
- Zusatzpakete:
  - opt/\*.txt Diese Dateien beschreiben, was bei welchen Einstellungen in das Archiv opt.img gelangt.
  - opt/... Optionale Kernel-Module, Dateien und Programme
- Quellcode:
  - src/\* Quellcode/Werkzeuge für Linux, siehe src/README
- Programme:
  - unix/mkfli4l\* Erzeugen des Bootmediums: Unix/Linux-Version
  - windows/\* Erzeugen des Bootmediums: Windows-Version
  - unix/imonc\* imond-Client für Unix/Linux
  - windows/imonc/\* imond-Client für Windows

## 2.2. Konfiguration

### 2.2.1. Editieren der Konfigurationsdateien

Zur Konfiguration von fli4l müssen lediglich die Dateien config/\*.txt angepasst werden. Um im Nachhinein die eigenen Konfiguration mit der ausgelieferten vergleichen zu können oder um mehrere Konfigurationen verwalten zu können, empfiehlt es sich, eine Kopie des config-Verzeichnisses anzulegen und die Konfiguration in dieser Kopie durchzuführen. Ein Vergleich der Konfigurationen ist dann durch Verwendung eines geeigneten Werkzeugs (z.B. “diff” unter \*nix) relativ einfach möglich. Nehmen wir einmal an, die eigene config liegt in einem Verzeichnis mit Namen “meine\_config” ebenfalls im fli4l-Verzeichnis dann wäre der Aufruf wie folgt:

```
~/src/fli4l> diff -u {config,meine_config}/build/rc.cfg | grep '^[+-]'
```

---	config/build/rc.cfg	2014-02-18 15:34:39.085103706	+0100
+++	meine_config/build/rc.cfg	2014-02-18 15:34:31.094317441	+0100

```
-PASSWORD='/P6h4i0IN5Bbc'
+PASSWORD='3P8F3KbjYgzUc'
-NET_DRV_1='ne2k-pci'
+NET_DRV_1='pcnet32'
-START_IMOND='no'
+START_IMOND='yes'
-OPT_PPPOE='no'
+OPT_PPPOE='yes'
-PPPOE_USER='anonymer'
-PPPOE_PASS='surfer'
+PPPOE_USER='ich'
+PPPOE_PASS='mein-passwd'
-OPT_SSHD='no'
+OPT_SSHD='yes'
```

Man sieht hier auch sehr schön, dass ein einfacher DSL-Router mit wenigen Handgriffen konfiguriert ist, auch wenn einen die Konfigurationsdateien auf den ersten Blick mit ihrer Fülle von Einstellungsmöglichkeiten erschlagen.

### 2.2.2. Konfiguration über eine spezielle Konfigurationsdatei

Da sich die Konfiguration durch das Modul-Konzept auf verschiedene Dateien verteilt, und das Bearbeiten dadurch unter Umständen etwas mühsam wird, kann man die Konfiguration auch in einer einzelnen Datei namens `<configverzeichnis>/_fli4l.txt` ablegen, deren Inhalt dann zusätzlich zu den normalen Konfigurationsdateien eingelesen wird und deren Inhalt dominiert. Um beim obigen Beispiel zu bleiben: Um einen einfachen DSL-Router zu konfigurieren, könnten wir einfach folgendes in diese Datei schreiben:

```
PASSWORD='3P8F3KbjYgzUc'
NET_DRV_N='1'
NET_DRV_1='pcnet32'
START_IMOND='yes'
OPT_PPPOE='yes'
PPPOE_USER='ich'
PPPOE_PASS='mein-passwd'
OPT_SSHD='yes'
```

Man sollte vermeiden, beide Konfigurationsvarianten zu mischen.

### 2.2.3. Variablen

Sie werden merken, dass einige Variablen auskommentiert sind. Wenn das der Fall ist, erhält sie eine sinnvolle Standard-Belegung. Diese Standard-Belegung ist für jede Variable dokumentiert. Wünschen Sie einen anderen Wert für diese Variable, sollten Sie das Kommentarzeichen am Anfang der Variablendefinition (`'#'`) entfernen und den entsprechenden Wert zwischen den Hochkommata einfügen.

## 2.3. Installationsvarianten

In den vorhergehenden Versionen von `fli4l` wurde lediglich das Booten von einer Diskette unterstützt. Dies ist aus oben genannten Gründen nun nicht mehr möglich, aber die Alternative mittels eines USB-Sticks ist gegeben.

Es sind auch eine Vielzahl anderer Bootmedien (CD, HD, Netzwerk, Compact-Flash, DoC, ...) möglich und `fli4l` kann auch auf diversen Medien installiert (HD, Compact-Flash, DoC) werden. Dazu kann `fli4l` auf drei verschiedenen Wegen gebootet werden:

**Single Image** Der Bootloader lädt den Linux-Kern und dann `fli4l` als ein einziges Image — danach kann `fli4l` ohne weiteren Zugriff auf andere Medien booten. Beispiele dafür sind die Boottypen *integrated*, *attached*, *netboot* und *cd*.

**Split Image** Der Bootloader lädt den Linux-Kern und dann ein rudimentäres `fli4l`-Image, dass die Bootmedien einbindet und die Konfiguration und restlichen Dateien aus einem dort liegenden Archiv holt. Beispiele dafür sind diese Boottypen: *hd (Typ A)*, *ls120*, *attached* und *cd-emul*.

**Installation auf einem Medium** Der Bootloader lädt den Linux-Kern und dann ein rudimentäres fli4l-Image, das eine bereits vorhandene fli4l-Installation in sein Dateisystem einbindet und damit keine weiteren Archive auspacken muss. Eine HD-Installation vom Typ B ist ein Beispiel dafür.

Man sollte jedoch zunächst erst einmal fli4l in einer minimalen Version installieren und damit Erfahrungen sammeln. Möchte man später fli4l zusätzlich als Anrufbeantworter und als HTTP-Proxy einsetzen, so hat man vorher schon mal Erfahrungen mit einem grundsätzlich laufenden Router.

Für die Installation ergeben sich daraus die folgenden fünf Varianten:

**USB-Stick** Router auf einem USB-Stick

**CD-router** Router auf einer CD

**Netzwerk** Netzwerkboot

**HD-Installation Typ A** Router auf Festplatte, CF, DoC – nur eine FAT-Partition

**HD-Installation Typ B** Router auf Festplatte, CF, DoC – je eine FAT- und ext3-Partition

### 2.3.1. Router auf einem USB-Stick

USB-Sticks werden von Linux als Festplatten angesprochen, daher gelten hier die Ausführungen zur Festplatteninstallation entsprechend. Bitte beachten Sie, dass mittels des `OPT_USB` die entsprechenden Treiber geladen werden müssen, damit der Stick mittels `OPT_HDINSTALL` eingebunden werden kann.

### 2.3.2. Router auf einer CD oder Netzwerkboot

Alle benötigten Dateien liegen auf dem Bootmedium und werden beim Booten in eine dynamische RAM-Disk entpackt. In einer Minimalkonfiguration ist damit ein Betrieb des Routers mit nur 64 MiB RAM möglich. Die maximale Konfiguration wird nur durch die Kapazität des Bootmediums und des Hauptspeichers limitiert.

### 2.3.3. Typ A: Router auf Festplatte – nur eine FAT-Partition

Dies entspricht der CD-version, nur dass die Dateien hierbei auf einer Festplatte liegen, wobei der Begriff „Festplatte“ hier auch Compact-Flash-Medien ab 8 MiB und andere Geräte, welche Linux als Festplatte ansprechen kann, mit einschließt. Seit fli4l 2.1.4 können auch DiskOnChip Flash-Speicher von M-Sys oder SCSI-Festplatten benutzt werden.

Die Beschränkung des Archivs `opt.img` durch die Diskettenkapazität wird aufgehoben, aber alle diese Dateien müssen in einer RAM-Disk mit der entsprechenden Größe beim Boot installiert werden. Dies erhöht den RAM-Bedarf beim Einsatz vieler Pakete.

Für ein Update der Softwarepakete (d.h. des Archivs `opt.img` und der `rc.cfg` über das Netzwerk) muss die FAT-Partition genügend Platz für den Kernel, das RootFS und die DOPPELTE Größe des `opt.img` haben! Falls auch die Notfall-Option genutzt werden soll, erhöht sich der Platzbedarf noch einmal um die Größe des `opt.img`.



#### **2.3.4. Typ B: Router auf Festplatte – je eine FAT- und ext3-Partition**

Im Gegensatz zum Typ A werden hier nicht alle Dateien in die Ramdisk gepackt, sondern bei dem erstmaligen Start nach der Installation oder nach einem Update aus dem Archiv `opt.img` direkt auf eine ext3-Partition kopiert und im späteren Betrieb von dort geladen. Bei dieser Version ist der Speicherbedarf für die RAM-Disk am geringsten und damit meist auch ein Betrieb mit sehr wenig RAM möglich.

Weitere Informationen zur Installation auf Festplatten finden Sie in der Dokumentation des Pakets `HD` (separat herunterzuladen)- beginnend bei der Beschreibung der Variablen `OPT_HDINSTALL`.

### 3. Basiskonfiguration

Ab Version 2.0 ist die fli4l-Distribution modular aufgebaut und in mehrere Pakete aufgeteilt, die extra heruntergeladen werden müssen. Im Paket `fli4l-4.0.0-trunk-rpi-r60784.tar.gz` ist lediglich die Basis-Software für einen Ethernet-Router enthalten. Für DSL, ISDN und weitere Software müssen die Pakete separat heruntergeladen werden und ausgehend vom Verzeichnis `fli4l-4.0.0-trunk-rpi-r60784/` (!) installiert werden. Durch die Auswahlmöglichkeit des Betriebssystemkerns von fli4l sind diese in die Kernel Pakete ausgelagert worden. Somit ist als Minimum Basis und ein Kernel Paket erforderlich. In Tabelle 3.1 finden Sie einen Überblick über die Zusatzpakete.

Die zur Konfiguration des fli4l-Routers verwendeten Dateien befinden sich im Verzeichnis `config/` und werden hier im Folgenden beschrieben.

Diese Dateien können mit einem *einfachen* Text-Editor oder auch mit einem speziell an fli4l angepassten Editor verändert werden. Diverse Editoren sind unter

<http://www.fli4l.de/download/zusatzpakete/addons/> zu finden.

Sind spezielle Anpassungen/Erweiterungen erforderlich, die über die unten aufgeführten Einstellungsmöglichkeiten hinausgehen, benötigt man ein lauffähiges Linux-System, um Anpassungen im RootFS vorzunehmen. In diesem Fall hilft `src/README` weiter.

### 3. Basiskonfiguration

Tabelle 3.1.: Übersicht über die (Zusatz-)Pakete

Download-Archiv	Paket
fli4l-4.0.0-trunk-rpi-r60784	BASIS, erforderlich!
kernel_4_19	Linux-Kernel, erforderlich!
fli4l-4.0.0-trunk-rpi-r60784-doc	Komplette Dokumentation
advanced_networking	Erweiterte Netzwerkkonfiguration
cert	Zertifikatsverwaltung
chrony	Time-Server/Client
dhcp_client	Verschiedene DHCP-Clients
dns_dhcp	DNS- und DHCP-Server
dslmodem	Unterstützung für interne DSL-Modems (z.B. AVM Fritz!DSL)
dyndns	Unterstützung von DYNDNS-Diensten
easycron	Zeitplandienst
hd	Installation auf Festplatte
httpd	Mini-Webserver für Status-Ausgaben
hwsupp	Unterstützung von Hardware
imonc_windows	Der Windows-Imonc
imonc_unix	Der GTK-Unix-Imonc
ipv6	Internet Protokoll Version 6
isdn	ISDN-Router
openvpn	OpenVPN-Unterstützung
pcmcia	Unterstützung von PCMCIA-Karten
ppp	PPP-Basispaket
pppoe	DSL-Router (PPPoE)
proxy	Proxy-Server
qos	Quality of Service
sshd	SSH-Server
tools	Diverse Linux-Werkzeuge
umts	Anbindung mittels UMTS an das Internet
usb	Unterstützung der USB-Schnittstelle
vpn	VPN (PPTP)
wlan	Unterstützung von WLAN-Karten

### 3.1. Beispiel-Datei

Die Beispiel-Datei `base.txt` im Verzeichnis `config/` hat folgenden Inhalt:

```
##-----
## fli4l __FLI4LVER__ - configuration for package "base"
##
## P L E A S E   R E A D   T H E   D O C U M E N T A T I O N !
##
## B I T T E   U N B E D I N G T   D I E   D O K U M E N T A T I O N   L E S E N !
##
##-----
```

### 3. Basiskonfiguration

```
## Creation:      26.06.2001  fm
## Last Update:  $Id: base.txt 60747 2022-09-15 11:47:18Z florian $
##
## Copyright (c) 2001-2016 - Frank Meyer, fli4l-Team <team@fli4l.de>
##
## This program is free software; you can redistribute it and/or modify
## it under the terms of the GNU General Public License as published by
## the Free Software Foundation; either version 2 of the License, or
## (at your option) any later version.
##-----

#-----
# General settings:
#-----
HOSTNAME='fli4l'           # name of fli4l router
PASSWORD='fli4l'          # password for root login (console, sshd,
                          # imond)
BOOT_TYPE='hd'            # boot device: hd, cd, ls120, integrated,
                          # attached, netboot, pxeboot
LIBATA_DMA='disabled'     # Use DMA on ATA Drives ('enabled') or not
                          # ('disabled'). The default 'disabled' allows
                          # ancient IDE CF cards to be booted from.
                          # Use 'enabled' if you boot from a VirtualBox's
                          # virtual device.
MOUNT_BOOT='rw'           # mount boot device: ro, rw, no
BOOTMENU_TIME='5'         # waiting time of bootmenu in seconds
                          # before activating normal boot
TIME_INFO='MEZ-1MESZ,M3.5.0,M10.5.0/3'
                          # description of local time zone,
                          # don't touch without reading documentation
RTC_SYNC='hwclock'        # how to synchronize the hardware clock?
KERNEL_VERSION='5.4.213'  # kernel version
KERNEL_BOOT_OPTION=''     # append option to kernel command line
COMP_TYPE_OPT='xz'        # compression algorithm if compression is
                          # enabled for OPT archive;
                          # NOTE that some boot types may disallow
                          # some compression algorithms
IP_CONNTRACK_MAX=''       # override maximum limit of connection
                          # tracking entries
POWERMANAGEMENT='acpi'    # select pm interface: none, acpi, apm, apm_rm
                          # apm_rm switches to real mode before invoking
                          # apm power off

#-----
# Localisation
#-----
LOCALE='de'               # defines the default language for several
                          # components, such as httpd

#-----
# Console settings (serial console, blank time, beep):
#-----
CONSOLE_BLANK_TIME=''     # time in minutes (1-60) to blank
```

### 3. Basiskonfiguration

```
# console; '0' = never, '' = system default
BEEP='yes' # enable beep after boot and shutdown
SER_CONSOLE='no' # use serial interface instead of or as
# additional output device and main input
# device
SER_CONSOLE_IF='0' # serial interface to use, 0 for ttyS0 (COM1)
SER_CONSOLE_RATE='9600' # baudrate for serial console

#-----
# Debug Settings:
#-----
DEBUG_STARTUP='no' # write an execution trace of the boot

#-----
# Keyboard layout
#-----
KEYBOARD_LOCALE='auto' # auto: use most common keyboard layout for
# the language specified in 'LOCALE'
#OPT_MAKEKBL='no' # set to 'yes' to make a new local keyboard
# layout map on the fli4l-router

#-----
# Ethernet card drivers:
#-----
#
# please see file base_nic.list in your config-dir or read the documentation
#
#
# If you need a dummy device, use 'dummy' as your NET_DRV
# and IP_NET_%_DEV='dummy<number>' as your device
#
#-----
#NET_DRV[]='ne2k-pci' # 1st driver: name (e.g. NE2000 PCI clone)
#{
# OPTION='' # 1st driver: additional option
#}
#NET_DRV[]='ne' # 2nd driver: name (e.g. NE2000 ISA clone)
#{
# OPTION='io=0x320' # 2nd driver: additional option
#}

#-----
# Network prefixes
#-----
#OPT_NET_PREFIX='no' # enable use of network prefixes: yes or no
#NET_PREFIX # network prefixes not bound to an interface
#{
# [] # network prefix assignment
# {
# NAME="site" # name of network prefix
# TYPE="static" # type of network prefix
# STATIC_IPv4="192.168.10.0/24" # static IPv4 prefix
# STATIC_IPv6="fd6e:d748:fd6d::/48" # static IPv6 prefix
```

### 3. Basiskonfiguration

```
# }
#}

#-----
# ULA prefixes
#-----
#OPT_NET_PREFIX_ULA='no'          # enable generation of ULAs: yes or no
#NET_PREFIX
#{
# []
# {
#   NAME="LAN"                    # name of network prefix
#   TYPE="generated-ula"          # type of network prefix
#   ULA_DEV='eth0'                # Ethernet interface of which the MAC is taken
# }
#}

#-----
# Networks
#-----
OPT_IPV4='yes'                    # enable IPv4 networking
                                  # WARNING: Don't set this to 'no', this is
                                  # currently not supported!

#IP_NET[1]='192.168.6.1/24'        # IP address of your n'th ethernet card and
                                  # netmask in CIDR (no. of set bits)

#{
#   DEV='eth0'                    # required: device name like ethX
#}

#OPT_IPV6='no'                    # set to 'yes' to activate IPv6 support

#IPV6_NET[1]='{internet-v6}+::1:0:0:0:1/64'
                                  # The router address and net mask of
                                  # this subnet. If this subnet is associated
                                  # with a circuit (i.e. the address is
                                  # prefixed by {<circuit>}), use an address
                                  # WITHOUT the subnet prefix; when the
                                  # associated circuit comes up, its prefix
                                  # will be combined with the address
                                  # specified here to yield a complete
                                  # address.
                                  #
                                  # NOTE that the net mask must be equal to
                                  # 64 if you want to use stateless IPv6
                                  # autoconfiguration!
                                  #
                                  # In this example, a /48 subnet prefix is
                                  # assumed which is extended by the subnet
                                  # '1' and the host part '0:0:0:1'. So with
                                  # e.g. '2001:db8:13bc/48' as subnet prefix
                                  # provided by circuit 'internet-v6', the
                                  # complete address and mask becomes
```

### 3. Basiskonfiguration

```
# '2001:db8:13bc:1::1/64'.
#
# If no circuit prefix is used, no circuit
# is associated, so the address
# specification is taken "as is" and is not
# completed by any prefix

#{
#  DEV='IP_NET_1_DEV'          # interface this subnet is bound to
#  ADVERTISE='yes'            # should the subnet prefix be advertised
#                             # automatically via RA in order to enable
#                             # stateless autoconfiguration?
#  ADVERTISE_DNS='no'         # should the DNS service be advertised
#                             # within this subnet via RA?
#}

#-----
# Additional routes, optional
#-----
#IP_ROUTE[]='192.168.7.0/24 192.168.6.99'
#                             # network/netmaskbits gateway
#IP_ROUTE[]='0.0.0.0/0 192.168.6.99'
#                             # example for default-route

#IPV6_ROUTE[]='2001:db8:13bc:2::/64 2001:db8:900:530::1'
#                             # example route

#-----
# Packet filter configuration
#-----
#-----
# INPUT chain
#-----
PF_INPUT_POLICY='REJECT'      # be nice and use reject as policy
PF_INPUT_ACCEPT_DEF='yes'     # use default rule set
PF_INPUT_LOG='no'             # don't log at all
PF_INPUT_LOG_LIMIT='3/minute:5' # log 3 events per minute; allow a burst of 5
#                             # events
PF_INPUT_REJ_LIMIT='1/second:5' # reject 1 connection per second; allow a burst
#                             # of 5 events; otherwise drop packet
PF_INPUT_UDP_REJ_LIMIT='1/second:5'
#                             # reject 1 udp packet per second; allow a burst
#                             # of 5 events; otherwise drop packet
#PF_INPUT[]='IP_NET_1 ACCEPT'  # allow all hosts in the local network to
#                             # access the router
#PF_INPUT[]='tmpl:samba DROP NOLOG'
#                             # drop (or reject) samba access

#{
#  COMMENT='no samba traffic allowed'
#                             # without logging, otherwise the log file will
#                             # be filled with useless entries
#}

PF6_INPUT_POLICY='REJECT'     # be nice and use reject as policy
```

### 3. Basiskonfiguration

```
PF6_INPUT_ACCEPT_DEF='yes'      # use default rule set
PF6_INPUT_LOG='no'              # don't log anything
PF6_INPUT_LOG_LIMIT='3/minute:5'
                                # log 3 events per minute; allow a burst of 5
                                # events
PF6_INPUT_REJ_LIMIT='1/second:5'
                                # reject 1 connection per second; allow a burst
                                # of 5 events; otherwise drop packet
PF6_INPUT_UDP_REJ_LIMIT='1/second:5'
                                # reject 1 udp packet per second; allow a burst
                                # of 5 events; otherwise drop packet

#PF6_INPUT[]='fe80::0/10] ACCEPT'
                                # allow all hosts in the local network to
                                # access the router
#PF6_INPUT[]='IPV6_NET_1 ACCEPT'
                                # allow all hosts in the first subnet to access
                                # the router
#PF6_INPUT[]='tmpl:samba DROP NOLOG'
                                # drop (or reject) samba access

#{
# COMMENT='no samba traffic allowed'
                                # without logging, otherwise the log file will
                                # be filled with useless entries
#}

#-----
# FORWARD chain
#-----
PF_FORWARD_POLICY='REJECT'      # be nice and use reject as policy
PF_FORWARD_ACCEPT_DEF='yes'     # use default rule set
PF_FORWARD_LOG='no'             # don't log at all
PF_FORWARD_LOG_LIMIT='3/minute:5'
                                # log 3 events per minute; allow a burst of 5
                                # events
PF_FORWARD_REJ_LIMIT='1/second:5'
                                # reject 1 connection per second; allow a burst
                                # of 5 events; otherwise drop packet
PF_FORWARD_UDP_REJ_LIMIT='1/second:5'
                                # reject 1 udp packet per second; allow a burst
                                # of 5 events; otherwise drop packet
#PF_FORWARD[]='tmpl:samba DROP' # drop samba traffic if it tries to leave the
                                # subnet
#PF_FORWARD[]='IP_NET_1 ACCEPT' # accept everything else

PF6_FORWARD_POLICY='REJECT'     # be nice and use reject as policy
PF6_FORWARD_ACCEPT_DEF='yes'    # use default rule set
PF6_FORWARD_LOG='no'           # don't log anything
PF6_FORWARD_LOG_LIMIT='3/minute:5'
                                # log 3 events per minute; allow a burst of 5
                                # events
PF6_FORWARD_REJ_LIMIT='1/second:5'
                                # reject 1 connection per second; allow a burst
```



### 3. Basiskonfiguration

```
# of 5 events; otherwise drop packet
PF6_FORWARD_UDP_REJ_LIMIT='1/second:5'
# reject 1 udp packet per second; allow a burst
# of 5 events; otherwise drop packet

#PF6_FORWARD[]='tmp1:samba DROP'
# drop samba traffic if it tries to leave the
# subnet
#PF6_FORWARD[]='IPV6_NET_1 ACCEPT'
# accept everything else

#-----
# OUTPUT chain
#-----
PF_OUTPUT_POLICY='ACCEPT'      # default policy for outgoing packets
PF_OUTPUT_ACCEPT_DEF='yes'     # use default rule set
PF_OUTPUT_LOG='no'             # don't log at all
PF_OUTPUT_LOG_LIMIT='3/minute:5'
# log 3 events per minute; allow a burst of 5
# events
PF_OUTPUT_REJ_LIMIT='1/second:5'
# reject 1 connection per second; allow a burst
# of 5 events; otherwise drop packet
PF_OUTPUT_UDP_REJ_LIMIT='1/second:5'
# reject 1 udp packet per second; allow a burst
# of 5 events; otherwise drop packet
#PF_OUTPUT[]='any 217.197.80.132 REJECT'
# don't allow the fli4l to reach fli4l.de

PF6_OUTPUT_POLICY='ACCEPT'     # default policy for outgoing packets
PF6_OUTPUT_ACCEPT_DEF='yes'    # use default rule set
PF6_OUTPUT_LOG='no'            # don't log anything
PF6_OUTPUT_LOG_LIMIT='3/minute:5'
# log 3 events per minute; allow a burst of 5
# events
PF6_OUTPUT_REJ_LIMIT='1/second:5'
# reject 1 connection per second; allow a burst
# of 5 events; otherwise drop packet
PF6_OUTPUT_UDP_REJ_LIMIT='1/second:5'
# reject 1 udp packet per second; allow a burst
# of 5 events; otherwise drop packet
#PF6_OUTPUT[]='any 2001:bf0:c000:a::2:132 REJECT'
# don't allow the fli4l to reach fli4l.de

#-----
# POSTROUTING chain
#-----
#PF_POSTROUTING[]='IP_NET_1 MASQUERADE'
# masquerade traffic leaving the subnet

#PF6_POSTROUTING[]='IPV6_NET_1 MASQUERADE'
# masquerade traffic leaving the subnet
```

### 3. Basiskonfiguration

```
#-----
# PREROUTING chain
#-----
#PF_PREROUTING[]='1.2.3.4 dynamic:22 DNAT:@client2'
# forward ssh connections coming from 1.2.3.4
# to client2

#PF6_PREROUTING[]='tmpl:ssh [2001:db8::1] DNAT:@client2'
# forward ssh connections coming from
# [2001:db8::1] to client2

#-----
# PREROUTING_CT chain
#-----
PF_PREROUTING_CT_ACCEPT_DEF='yes'
# use default rule set
#PF_PREROUTING_CT[]='tmpl:ftp IP_NET_1 HELPER:ftp'
# associate FTP conntrack helper for active FTP
# forwarded from within the LAN to some FTP
# server outside
#PF_PREROUTING_CT[]='tmpl:ftp any dynamic HELPER:ftp'
# associate FTP conntrack helper for passive
# FTP forwarded to the router's external IP
# (some PREROUTING rule needs to forward the
# packets to some FTP server within the LAN)

#PF6_PREROUTING_CT[]='tmpl:ftp IPV6_NET_1 HELPER:ftp'
# associate FTP conntrack helper for active FTP
# forwarded from within the LAN to some FTP
# server outside
#PF6_PREROUTING_CT[]='tmpl:ftp any IPV6_NET_1 HELPER:ftp'
# associate FTP conntrack helper for passive
# FTP forwarded to some FTP server within the
# LAN

#-----
# OUTPUT_CT chain
#-----
PF_OUTPUT_CT_ACCEPT_DEF='yes' # use default rule set
#PF_OUTPUT_CT[]='tmpl:ftp HELPER:ftp'
# associate FTP conntrack helper for outgoing
# active FTP on the router (this rule is added
# automatically by the tools package if
# OPT_FTP='yes' and FTP_PF_ENABLE_ACTIVE='yes')

#PF6_OUTPUT_CT[]='tmpl:ftp HELPER:ftp'
# associate FTP conntrack helper for outgoing
# active FTP on the router (this rule is added
# automatically by the tools package if
# OPT_FTP='yes' and FTP_PF_ENABLE_ACTIVE='yes')

#-----
# USER chain
```

### 3. Basiskonfiguration

```
#-----
#PF_USR_CHAIN[]='...'          # some user-defined rule
#PF6_USR_CHAIN[]='...'         # some user-defined rule

#-----
# Domain configuration:
# settings for DNS, DHCP server and HOSTS -> see package DNS_DHCP
#-----
DOMAIN_NAME='lan.fli4l'        # your domain name
DNS_FORWARDERS='194.8.57.8'    # DNS servers of your provider,
                                # e.g. ns.n-ix.net

# optional configuration for the host-entry of the router in /etc/hosts
#HOSTNAME_IP='IP_NET_1_IPADDR' # IP to bind to HOSTNAME
#HOSTNAME_IP6='IPV6_NET_1_IPADDR'
                                # optional, can be used to explicitly set
                                # the router's IPv6 address; if left empty,
                                # this setting is taken from the first
                                # configured /64 IPv6 subnet (see below)
#HOSTNAME_ALIAS[]='router.lan.fli4l'
                                # first ALIAS name
#HOSTNAME_ALIAS[]='gateway.my.lan'
                                # second ALIAS name

#-----
# optional package: syslogd
#-----
#OPT_SYSLOGD='no'              # start syslogd: yes or no
#SYSLOGD_RECEIVER='yes'        # receive messages from network
#SYSLOGD_DEST[]='*. * /dev/console'
                                # n'th prio & destination of syslog msgs
#SYSLOGD_DEST[]='*. * @192.168.6.2'
                                # example: loghost 192.168.6.2
#SYSLOGD_DEST[]='kern.info /var/log/dial.log'
                                # example: log infos to file

SYSLOGD_ROTATE='no'            # rotate syslog-files once every day
SYSLOGD_ROTATE_DIR='/data/syslog'
                                # move rotated files to ....
SYSLOGD_ROTATE_MAX='5'        # max number of rotated syslog-files

#-----
# Optional package: klogd
#-----
#OPT_KLOGD='no'                # start klogd: yes or no

#-----
# Optional package: logip
#-----
#OPT_LOGIP='no'                # logip: yes or no
LOGIP_LOGDIR='auto'            # log-directory, e.g. /boot or auto-detected

#-----
```

### 3. Basiskonfiguration

```
# Optional package: y2k correction
#-----
#OPT_Y2K='no'                # y2k correction: yes or no
Y2K_DAYS='0'                 # correct hardware y2k-bug: add x days

#-----
# Optional package: PNP
#-----
#OPT_PNP='no'                # install isapnp tools: yes or no

#-----
# Optional: PCI hotplugging
#-----
#OPT_HOTPLUG_PCI='no'        # if yes, various PCI hotplugging drivers are
                             # loaded at boot time; note that ACPI hot-
                             # plugging (as used by e.g. KVM) is built into
                             # the kernel and does _not_ require this OPT to
                             # be enabled (but it doesn't hurt neither)

#-----
# Optional package: lua
# (Note: This package will eventually be integrated into the base package as
# it is planned to implement core fli4l services in Lua!)
#-----
#OPT_LUA='no'                # enable Lua

#-----
# Optional package: luatests
#-----
#OPT_LUATESTS='no'          # enable Lua test suite
#LUATESTS_RUNATBOOTTIME='yes' # set to 'yes' if test suite should run when
                             # the fli4l boots
```

Zu beachten ist, dass diese Datei im DOS-Format gespeichert ist. Das heißt, sie enthält jeweils am Zeilenende ein zusätzliches Carriage-Return (CR). Da die meisten Unix-Editoren damit keine Probleme bekommen wurde dieses Format gewählt, denn umgekehrt hat der Windows-Editor bei fehlendem CR am Zeilenende keine Chance!

Sollte es wider Erwarten unter Unix/Linux doch Probleme mit dem Lieblingseditor geben, kann die Datei vor dem Editieren mit einem Befehl in das Unix-Format konvertiert werden:

```
sh unix/dtou config/base.txt
```

Für die Erstellung des Boot-Mediums ist es völlig unerheblich, ob die Datei CRs am Zeilenende enthält oder nicht. Sie werden beim Schreiben auf das Boot-Medium einschließlich der Kommentare komplett ignoriert.

Jetzt aber zum Inhalt ...

## 3.2. Allgemeine Einstellungen

**HOSTNAME** Standardwert: `HOSTNAME='fli4l'`

Als erstes sollte man seinem fli4l-Router einen Namen geben.

**PASSWORD** Standardwert: `PASSWORD='fli4l'`

Das hier angegebene Passwort wird für das Einloggen in den fli4l-Rechner benötigt – sei es per Tastatur direkt am Router oder per SSH von einem anderen Rechner aus (hierzu wird das `sshd`-Paket benötigt). Es muss aus mindestens einem und darf aus höchstens 126 Zeichen bestehen.

**BOOT\_TYPE** Standardwert: `BOOT_TYPE='hd'`

`BOOT_TYPE` legt im weitesten Sinne das Bootmedium fest. Diese Variable steuert, welche zusätzlichen Treiber (Kernel-Module) und Start-Skripte mit in das RootFS aufgenommen werden. Zum Verständnis eine kurze Skizze des Bootvorgangs:

- Das BIOS des Rechners lädt/startet den Bootloader auf dem Bootmedium.
- Der Bootloader (i.d.R. `syslinux`) entpackt, lädt und startet den Kernel.
- Der Kernel entpackt das RootFS (= das grundlegende Dateisystem mit darin enthaltenen Programmen und Skripten), mountet das RootFS und beginnt die Start-Skripte abzuarbeiten.
- Je nach `BOOT_TYPE` werden nun die Kernel-Module für das jeweilige Bootmedium geladen, die Boot-Partition gemountet und das OPT-Archiv (`opt.img`) mit den zusätzlichen Programmen entpackt.
- Im Anschluss beginnt die Konfiguration der einzelnen Dienste des fli4l.

Zur Zeit sind folgende Werte für `BOOT_TYPE` gültig:

**ls120** Boot von LS120/240 sowie ZIP Disks.

**hd** Boot von Festplatte. IDE und SATA Geräte werden direkt erkannt, für SCSI, USB oder besondere Controller wird das Paket `HD` und/oder `USB` benötigt. Näheres ist der [Dokumentation](#) (Seite 158) zum Paket `HD` zu entnehmen.

**cd** Boot von CD-ROM. Es wird lediglich das ISO-Image `fli4l.iso` der CD erzeugt, welches anschließend mit dem jeweiligen Lieblingsbrennprogramm selbst auf CD gebrannt werden muss. Bezüglich SCSI, USB und spezielle Controller ist das Paket `HD` bzw. `USB` nötig.

**integrated** Bei diesem Typ wird kein Bootmedium zu Grunde gelegt, sondern das OPT-Archiv vollständig ins RootFS integriert. Somit entfällt das Mounten des Bootmediums und der Kernel kann gleich alles entpacken. Dieser `BOOT_TYPE` wird z.B. fürs Booten vom Netzwerk benötigt.

**Hinweis:** Ein remote Update ist natürlich in diesem Fall nicht möglich.

**attached** Ähnlich wie **integrated**, jedoch wird das OPT-Archiv als Datei `opt.img` ans RootFS angehängt, mit der Folge, dass es wieder im Verzeichnis `/boot` zu finden ist und gesondert beim Bootvorgang entpackt wird.

Ansonsten gilt das unter **integrated** Gesagte.

**netboot** Entspricht **integrated**. Es wird jedoch zusätzlich das Skript `mknetboot.sh` gestartet, welches ein Image zum Booten via LAN erzeugt. Weiteres ist bitte dem Wiki <https://ssl.networks.org/wiki/display/f/fli4l+und+Netzboot> zu entnehmen.

### 3. Basiskonfiguration

**pxeboot** Es werden zwei Images generiert, kernel und rootfs.img. Das sind die beiden vom PXE-Bootloader nachzuladenden Dateien. Beim Aufruf kann die Location des tftp-Verzeichnisses angegeben werden und zusätzlich noch ein Unterverzeichnis innerhalb des tftp-Verzeichnisses (-pxesubdir). Weiteres auch hier im Wiki <https://ssl.networks.org/wiki/display/f/fli4l+und+Netzboot>

**Hinweis:** wie ein fli4l als passender boot-server (pxe/tftp) zu konfigurieren ist, können sie in der Dokumentation des Pakets dns\_dhcp nachlesen.

**LIBATA\_DMA** Mit dieser Variable kann eingestellt werden, ob DMA für libata basierte Geräte aktiviert werden soll. Dies ist z.B. bei einigen unvollständig verdrahteten IDE zu Compact-Flash Adaptern nötig. Um DMA zu aktivieren: 'enabled' Default: 'disabled'

**MOUNT\_BOOT** Standardwert: MOUNT\_BOOT='rw'

Hier wird eingestellt, wie das Boot-Medium gemountet werden soll. Es gibt drei Möglichkeiten:

**rw** – Read/Write – Schreiben und Lesen ist möglich

**ro** – Read-Only – Nur Lesen ist möglich

**no** – None – Medium wird nach dem Boot wieder abgemeldet und kann dann bei Bedarf entnommen werden.

Bei bestimmten Konfigurationen ist es unbedingt erforderlich, das Medium Read/Write anzumelden, z.B. wenn man den DHCP-Server einsetzen oder die imond-Log-Datei auf dem Medium anlegen möchte.

**BOOTMENU\_TIME** Standardwert: BOOTMENU\_TIME='20'

Hier wird eingestellt, wie lange der syslinux Bootloader warten soll, bis automatisch mit der Standard-Installation gebootet wird.

Im Paket HD besteht die Möglichkeit, über OPT\_RECOVER eine Funktion zu aktivieren, mit der eine Notfallinstallation aus einer laufenden Installation erstellt werden kann. Diese kann im Bootmenü über die Wahl der Recover-Version aktiviert werden.

Sollte hier der Wert '0' eingestellt sein, wartet der syslinux Bootloader bis der Anwender die Standard- oder die Recover-Version auswählt und aktiviert!

**TIME\_INFO** Standardwert: TIME\_INFO='MEZ-1MESZ,M3.5.0,M10.5.0/3'

Uhren ticken in der Unix-Welt und damit auch unter fli4l normalerweise nach der UTC (Universal Time Coordinated), einer weltweit einheitlichen Uhrzeit, die vor der Verwendung in die lokale Zeit umgerechnet wird. TIME\_INFO liefert fli4l die dafür notwendigen Informationen über die Namen der Zeitzonen, die Differenz zu UTC und Regeln, wann auf Sommerzeit und wieder zurück gewechselt wird. Damit das korrekt funktioniert, muss die Hardware Uhr auf UTC gestellt werden (entspricht der Londoner Winterzeit) oder über das Paket chrony mit einem Timeserver synchronisiert werden (diese liefern UTC aus).

Die Einträge in TIME\_INFO bedeuten dabei folgendes:

### 3. Basiskonfiguration

```
TIME_INFO='MEZ-1MESZ,M3.5.0,M10.5.0/3'
```

- *MEZ-1*: Wir befinden uns in der mitteleuropäischen Zeitzone (*MEZ*), die der UTC eine Stunde voraus ist  $MEZ-1=UTC$ .
- *MESZ*: In dieser Zeitzone gibt es Sommerzeit (Mittleuropäische Sommerzeit). Da nichts weiter angegeben wird, kommt man zur Sommerzeit, indem man die Zeit eine Stunde vorstellt.
- *M3.5.0,M10.5.0/3*: Am letzten Sonntag im März (um 2 Uhr) wird zur Sommerzeit gewechselt, am letzten Sonntag im Oktober (um 3 Uhr) wieder zurück.

Normalerweise braucht man diesen Wert nie anzufassen, es sei denn man sitzt in einer anderen Zeitzone. Will man die Werte anpassen, sollte man einen Blick auf die Spezifikation der Umgebungsvariable TZ werfen, die unter folgender URL zu finden ist (englisch): [http://pubs.opengroup.org/onlinepubs/009695399/basedefs/xbd\\_chap08.html](http://pubs.opengroup.org/onlinepubs/009695399/basedefs/xbd_chap08.html)

**RTC\_SYNC** Standardwert: `RTC_SYNC='hwclock'`

In vielen Rechnern steckt eine batteriegepufferte Hardware-Uhr, die auch über die Dauer der Abschaltung mit Strom versorgt wird und die Uhrzeit weiterzählt, so dass sie beim nächsten Starten wieder als Systemzeit zur Verfügung steht. Es ist an dieser Stelle wichtig, zwischen der *Systemzeit* und der *Hardwarezeit* zu unterscheiden:

- Die *Hardwarezeit* ist die Zeit, die in der Hardware-Uhr gespeichert und von dieser aktuell gehalten wird. Sie wird in der Regel beim Starten des Systems aus der Hardware-Uhr ausgelesen und als Systemzeit übernommen.
- Die *Systemzeit* ist die eigentliche Zeit, die das Linux-System verwendet und z. B. beim Aufruf des Befehls `date -u` angezeigt wird. Sie wird vom Linux-Kernel aktuell gehalten, etwa auf Basis regelmäßiger Hardware-Unterbrechungen (Timer-Interrupt), bezeichnet immer einen Zeitpunkt in koordinierter Weltzeit (UTC), und wird nicht von der Zeitzone-Einstellung beeinflusst.
- Die *lokalisierte Systemzeit* ist lediglich die Umrechnung der Systemzeit in eine andere Zeitzone, die auf dem fli4l-Router über die Umgebungsvariable TZ konfiguriert wird (siehe die Variable `TIME_INFO` (Seite 30)), und spielt im weiteren Verlauf dieses Abschnitts keine Rolle.

Mit Hilfe dieser Variable wird dem fli4l mitgeteilt, wie der Abgleich der Hardwarezeit mit der Systemzeit vorgenommen werden soll, d. h. ob und wie oft die Hardwarezeit auf die Systemzeit gesetzt werden soll. Ein solcher Abgleich ist nötig, weil auch die beste Hardware-Uhr nicht zu 100 % genau geht und zum systematischen Abdriften neigt, d. h. sie geht auf Dauer gesehen etwas zu langsam oder etwas zu schnell.

Es gibt prinzipiell zwei Möglichkeiten der Synchronisation:

- Modus "kernel": Ein NTP-Client wird verwendet, um von außen (in der Regel über das Internet oder eine externe (Funk-)Uhr) die tatsächliche Uhrzeit zu ermitteln und die Systemzeit des fli4l-Routers aktuell zu halten. Dabei wird der Linux-Kernel angewiesen, sich um die Aktualisierung der Hardwarezeit zu kümmern, so dass keine weitere Synchronisierung mehr nötig ist. Die Aktualisierung durch den Linux-Kernel

### 3. Basiskonfiguration

ist etwas weniger genau als die Aktualisierung mittels **hwclock** (siehe Modus “hwclock” weiter unten), allerdings ist die Güte der Aktualisierung weit weniger wichtig, weil der zwangsläufige Fehler durch den NTP-Client ausgeglichen wird.

Dieser Modus muss auch verwendet werden, wenn gar keine Hardware-Uhr existiert. Der Linux-Kernel wird in diesem Falle natürlich keine Hardwarezeit aktuell halten, weil es keine gibt. Es sollte dann allerdings unbedingt ein NTP-Client verwendet werden, damit der fli4l-Router überhaupt eine sinnvolle Systemzeit erhält.

- Modus “hwclock”: Es findet beim Herunterfahren des Systems (bei der Ausführung des Stopp-Skripts `/etc/rc0.d/rc950.hwclock`) sowie in regelmäßigen Abständen (alle 24 Stunden) eine Synchronisation mit Hilfe des **hwclock**-Programms statt. Dabei wird nicht nur die Hardwarezeit gesetzt, sondern **hwclock** misst auch, inwieweit die Systemzeit von der Hardwarezeit abweicht. Beim Starten des Systems wird dann die Systemzeit nicht direkt aus der Hardwarezeit übernommen, sondern es wird auch die Abweichung berücksichtigt, um das Abdriften der Systemzeit möglichst zu reduzieren. Die Abweichung wird in der Datei `/etc/adjtime` vermerkt. Ist ein beschreibbares persistentes Medium verfügbar, wird die Abweichung unter `/var/lib/persistent/base/adjtime` gespeichert; in diesem Falle ist `/etc/adjtime` eine symbolische Verknüpfung dorthin.

Dieser Modus ist inkompatibel zu einer Aktualisierung der Systemzeit mit Hilfe eines NTP-Clients. Das liegt daran, dass ein NTP-Client automatisch das Aktualisieren der Hardwareuhr durch den Linux-Kernel aktiviert. Es ist jedoch wenig sinnvoll bzw. problematisch, dass sowohl **hwclock** als auch der Linux-Kernel gleichzeitig versuchen, die Hardwarezeit aktuell zu halten.

Es ist zu beachten, dass wenn eine Hardware-Uhr zur Verfügung steht, die darin gespeicherte Uhrzeit *immer* als koordinierte Weltzeit (UTC) interpretiert wird. Die Zeitzone, die über die Variable `TIME_INFO` gesetzt wird, wirkt sich nicht auf die in der Hardware-Uhr gespeicherte Zeit aus. Das Speichern einer lokalisierten Nicht-UTC-Zeit in der Hardware-Uhr wird von fli4l *nicht* unterstützt.

Das Ermitteln der Systemzeit aus der Hardwarezeit wird einmalig beim Starten des Systems vorgenommen. Dabei wird bereits durch den Linux-Kernel das Auslesen der Hardware-Uhr und das Setzen der Systemzeit unmittelbar am Beginn des Bootvorgangs vorgenommen. Im Modus “hwclock” wird dann später bei der Ausführung des Boot-Skripts `/etc/rc.d/rc100.hwclock` die Systemzeit erneut gesetzt, diesmal unter Berücksichtigung der systematischen Abweichung.

**KERNEL\_VERSION** Legt die Version des zu verwendenden Kerns fest. Entsprechend dieser Variable werden der Kern aus `img/kernel-<kernel version>.<compression extension>` und die Kernel-Module aus `opt/lib/modules/<kernel version>` selektiert.

**KERNEL\_BOOT\_OPTION** Standardwert: `KERNEL_BOOT_OPTION=""`

Der Inhalt dieser Variable wird an die Kommandozeile des Kerns in der `syslinux.cfg` angehängt. Manche Systeme benötigen für korrekten Reboot `'reboot=bios'`. Bei WRAP-Systemen also `'reboot=bios'`.

**COMP\_TYPE\_ROOTFS** Standardwert: `COMP_TYPE_ROOTFS='xz'`



### 3. Basiskonfiguration

Der Inhalt dieser Variable legt die Kompressionsmethode für das RootFS-Archiv fest. Mögliche Werte sind 'xz', 'lzma' und 'bzip2'.

**COMP\_TYPE\_OPT** Standardwert: `COMP_TYPE_OPT='xz'`

Der Inhalt dieser Variable legt die Kompressionsmethode für das OPT-Archiv fest. Mögliche Werte sind 'xz', 'lzma' und 'bzip2'.

**POWERMANAGEMENT** Standardwert: `POWERMANAGEMENT='acpi'`

Der Kern unterstützt verschiedene Formen des Powermanagements, das etwas betagte APM und das aktuellere ACPI. Hier kann man einstellen, welche Form er verwenden soll. Mögliche Werte sind 'none' (kein Powermanagement), 'acpi' und die beiden APM-Varianten 'apm' und 'apm\_rm'. Letzteres schaltet in einen speziellen Prozessormodus, bevor der Router ausgeschaltet wird.

**FLI4L\_UUID** Standardwert: `FLI4L_UUID=""`

Hier wird eine eindeutige UUID eingetragen, mit der der fli4l seine persistenten Daten auf z.B. einem USB-Stick finden kann. Eine UUID kann auf einem beliebigen Linux-System (wie auch dem fli4l) mit dem Befehl `'cat /proc/sys/kernel/random/uuid'` erstellt werden. Dies gibt bei jedem Aufruf eine neue UUID aus. Diese muss nun in die Variable eintragen werden. Auf einem persistenten Medium (z.B. auf einer Festplatte (OPT\_HD) oder einem USB-Stick (OPT\_USB und OPT\_HD)) muss dann noch ein Verzeichnis mit demselben Namen angelegt werden. Dort wird dann künftig alles gespeichert, das sich gegenüber der Konfiguration geändert hat, ebenso wie persistente Laufzeitdaten wie z.B. DHCP-Leases. Hierzu muss das entsprechende Paket dies natürlich unterstützen (siehe Dokumentation). Der entsprechende Eintrag für den Speicherpfad ist dort dann in der Regel 'auto'.

Sollte der fli4l bereits vor dem Erstellen der UUID und dem Anlegen des Verzeichnisses einige Daten gespeichert haben, so sind diese unter /boot/persistent zu finden und müssen dann manuell an den neuen Speicherort verschoben werden. Deshalb empfiehlt es sich, die UUID gleich anfangs zu erstellen und nicht erst später zu migrieren.

Zudem ist zu beachten, dass `MOUNT_BOOT='ro'` nicht gewählt werden darf, solange das Verzeichnis sich irgendwo auf der /boot Partition befindet.

Ein empfohlener Ort für das persistente Verzeichnis befindet sich auf der /data Partition (ganz oben) oder einem USB-Stick. Das Dateisystem des USB-Sticks sollte VFAT sein oder bei aktivem OPT\_HD alle dort unterstützen schreib-lese-fähigen Dateisysteme.

**IP\_CONNTRACK\_MAX** Standardwert: `IP_CONNTRACK_MAX=""`

Mit Hilfe dieser Variable kann man die maximale mögliche Anzahl gleichzeitiger Verbindungen manuell einstellen. Normalerweise wird anhand des eingebauten Arbeitsspeichers automatisch ein sinnvoller Wert ermittelt. In Tabelle 3.2 sind die verwendeten Voreinstellungen zusammengefasst dargestellt.

Bei Einsatz von FileSharing-Programmen hinter oder auf dem Router und wenig Arbeitsspeicher ist die maximale Anzahl gleichzeitiger Verbindungen aber sehr schnell erreicht und zusätzliche Verbindungen können nicht mehr aufgebaut werden.

Das äußert sich in Fehlermeldungen wie

### 3. Basiskonfiguration

Tabelle 3.2.: Automatische Einstellung der maximalen Verbindungsanzahl

Arbeitsspeicher in MiB	gleichzeitige Verbindungen
16	1024
24	1280
32	2048
64	4096
128	8192

```
ip_conntrack: table full, dropping packet
```

oder

```
ip_conntrack: Maximum limit of XXX entries exceeded
```

Mittels `IP_CONNTRACK_MAX` lässt sich nun die maximale Anzahl gleichzeitiger Verbindungen fest auf einen bestimmten Wert einstellen. Jede einzelne mögliche Verbindung kostet 350 Bytes Arbeitsspeicher, der nicht mehr für andere Dinge genutzt werden kann. Setzt man also 10000, so sind gerundet 3,34 MB Arbeitsspeicher für den normalen Gebrauch verloren (Kernel, Ramdisks, Programme).

Bei 32 MiB RAM sollte es kein Problem sein, mal eben 2 oder 3 MiB für die `ip_conntrack`-Tabelle zu reservieren, bei 16 MiB wird es knapp und bei 12 oder sogar 8 MiB ist absolute Sparwut angesagt.

Die momentan benutzte Einstellung lässt sich auf der Konsole mit

```
cat /proc/sys/net/ipv4/ip_conntrack_max
```

anzeigen und mit

```
echo "XXX" > /proc/sys/net/ipv4/ip_conntrack_max
```

zur Laufzeit setzen, wobei XXX für die Anzahl der Einträge steht. Die Einträge in der `IP_CONNTRACK`-Tabelle selbst können auf der Konsole mit

```
cat /proc/net/ip_conntrack
```

angesehen und mit

```
cat /proc/net/ip_conntrack | grep -c use
```

gezählt werden.

**LOCALE** Standardwert: `LOCALE='de'`

Einige Komponenten sind mittlerweile mehrsprachfähig. Dazu zählen beispielsweise das Konsolen-Menü und die Weboberfläche. Mit dieser Variablen können Sie die bevorzugte Sprache auswählen. Verschiedene Komponenten haben noch eine eigene Einstellung womit diese Grundeinstellung, wenn nötig, überlistet werden kann. Wenn die hier angegebene Sprache bei einer Komponente (noch) nicht verfügbar ist, wird auf Englisch zurückgefallen.

Bei `KEYBOARD_LOCALE='auto'` wird versucht ein zu der `LOCALE`-Einstellung passendes Tastatur-Layout ein zu stellen.

Bisher sind folgende Einstellungen möglich: de, en, es, fr, hu, nl.

### 3.3. Konsolen-Einstellungen

fli4l kann auf verschiedenen Hardware-Plattformen betrieben werden. Auf vielen dieser Plattformen ist es möglich, eine Tastatur und einen Monitor anzuschließen, um mit dem fli4l zu interagieren; diese Kombination der Ein- und Ausgabe wird generell *Konsole* genannt.

fli4l kann aber auch gänzlich ohne Tastatur und Grafikkarte eingesetzt werden. Damit man den Router dann auch ohne Netzwerkzugriff bedienen sowie alle Boot-Meldungen des Kernels sehen kann, ist es u. a. möglich, über die serielle Schnittstelle ebenfalls eine Konsole zu erhalten, indem die Ein- und Ausgaben von der serielle Schnittstelle bezogen bzw. dorthin ausgegeben werden. Dazu müssen die Variablen `SER_CONSOLE` (Seite 35), `SER_CONSOLE_IF` (Seite 36) und `SER_CONSOLE_RATE` (Seite 36) gesetzt bzw. angepasst werden.

Schließlich ist es möglich, zur selben Zeit sowohl über Tastatur und Monitor als auch über die serielle Schnittstelle eine Konsole zur Verfügung zu stellen.

Generell stellt fli4l auf *jeder* Konsole die Möglichkeit zur Anmeldung und somit eine *Shell* zur Verfügung, an der Sie sich mit dem Benutzer “fli4l” und dem über die Variable `PASSWORD` (Seite 29) konfigurierten Passwort anmelden können.

**CONSOLE\_BLANK\_TIME** Standard-Einstellung: `CONSOLE_BLANK_TIME=""`

Normalerweise aktiviert der Linux-Kern nach einer gewissen Zeit ohne Eingaben auf dem aktuellen Eingabegerät den Bildschirmschoner. Mit der Variable `CONSOLE_BLANK_TIME` kann man diese Zeit konfigurieren bzw. den Bildschirmschonermodus ganz deaktivieren (`CONSOLE_BLANK_TIME='0'`).

**BEEP** Standard-Einstellung: `BEEP='yes'`

Signalton am Ende des Boot- und Shutdownprozesses ausgeben.

Trägt man hier ‘yes’ ein, ertönt ein Signalton am Ende des Boot- und Shutdownprozesses. Wer extremen Platzmangel auf dem Bootmedium hat oder keinen Signalton möchte, kann hier also ‘no’ eingetragen lassen.

**SER\_CONSOLE** Standard-Einstellung: `SER_CONSOLE='no'`

Diese Variable aktiviert oder deaktiviert eine Konsole auf einer seriellen Schnittstelle. Die serielle Konsole kann in drei Modi betrieben werden:

### 3. Basiskonfiguration

SER_CONSOLE	Konsolen-Ein-/Ausgabe
no	Ein- und Ausgabe (nur) über Tastatur und Monitor (tty0)
yes	Ein- und Ausgabe (nur) über serielle Schnittstelle (ttyS0)
primary	Ein- und Ausgabe sowohl über serielle Konsole als auch über Tastatur und Monitor, Ausgabe der Kernelmeldungen auf tty0
secondary	Ein- und Ausgabe sowohl über serielle Konsole als auch über Tastatur und Monitor, Ausgabe der Kernelmeldungen auf ttyS0

Wenn der Wert von `SER_CONSOLE` verändert wird, wird diese Änderung nur bei der Erstellung eines neuen Bootmediums oder beim Remote-Update der `syslinux.cfg` wirksam.

**Wichtig:** Achten Sie beim Ausschalten der seriellen Konsole darauf, sich einen alternativen Zugang zum Router (SSH oder direkt über Tastatur und Monitor) zu erhalten!

Weitere Informationen sind im Anhang unter [Serielle Konsole](#) (Seite 404) zu finden.

**SER\_CONSOLE\_IF** Standard-Einstellung: `SER_CONSOLE_IF='0'`

Nummer der seriellen Schnittstelle für die serielle Konsole.

Hier ist die Nummer der Schnittstelle einzutragen, an die die serielle Konsole angeschlossen wird. 0 entspricht ttyS0 unter Linux bzw. COM1 unter Microsoft Windows.

**SER\_CONSOLE\_RATE** Standard-Einstellung: `SER_CONSOLE_RATE='9600'`

Übertragungsrate der seriellen Schnittstelle für die Konsolenausgabe.

Hier trägt man die Baud-Rate ein, mit der die Daten auf der seriellen Schnittstelle übertragen werden. Sinnvolle Werte: 4800, 9600, 19200, 38400, 57600, 115200.

## 3.4. Hilfen zum Einkreisen von Problemen und Fehlern

fli4l loggt die gesamten Ausgaben des Bootvorganges in einer Datei (`/var/tmp/boot.log`). Diese Datei kann man sich am Ende des Bootvorganges auf der Konsole oder über den entsprechenden Menüpunkt im Web-Interface ansehen.

Manchmal ist es jedoch sinnvoll, bei Problemen einen ausführlicheren Ablauf der Start-Sequenz zu generieren, um den Bootvorgang hinterher auf Probleme untersuchen zu können. Dazu dient `DEBUG_STARTUP`. Andere Einstellungen unterstützen Entwickler beim Finden von Fehlern in bestimmten Situationen; auch diese Einstellungen werden in diesem Abschnitt dokumentiert.

**DEBUG\_STARTUP** Standard-Einstellung: `DEBUG_STARTUP='no'`

Steht dieser Wert auf 'yes', wird beim Booten jedes ausgeführte Kommando vor seiner Ausführung auf den Schirm geschrieben. Da für das korrekte Funktionieren Änderungen an der `syslinux.cfg` vorgenommen werden müssen, gilt das für `SER_CONSOLE` Gesagte auch hier. Wenn man die `syslinux.cfg` von Hand ergänzen will, ist es nötig, ein `fli4ldebug=yes` einzufügen. `DEBUG_STARTUP` muss dann aber trotzdem auf 'yes' stehen.

**DEBUG\_MODULES** Standard-Einstellung: `DEBUG_MODULES='no'`

Einige Module werden automatisch vom Kern geladen, ohne dass man das vorher erkennen kann. `DEBUG_MODULES='yes'` aktiviert einen Modus, der einem die kompletten Modul-ladesequenzen zeigt, egal, ob sie von einem Skript oder vom Kern angestoßen werden.

**DEBUG\_ENABLE\_CORE** Standard-Einstellung: `DEBUG_ENABLE_CORE='no'`

Wird diese Option aktiviert, verursacht jeder Programmabsturz auf dem Router das Erzeugen einer so genannten “core”-Datei, also eines Speicherabbilds des Prozesses direkt vor dem Absturz. Diese Dateien sind auf dem Router im Verzeichnis `/var/log/dumps` zu finden. Diese Dateien können dann genutzt werden, um den Programmfehler besser zu finden. Genauer finden Sie hierzu im Abschnitt [“Entwanzen von Programmen auf dem fli4l”](#) (Seite 298) in der Dokumentation des SRC-Pakets.

**DEBUG\_MDEV** Standard-Einstellung: `DEBUG_MDEV='no'`

Mit `DEBUG_MDEV='yes'` werden alle Aktionen, die in Zusammenhang mit dem `mdev`-Dämon stehen und somit mit dem Hinzufügen oder Entfernen von Geräteknoten in `/dev` oder dem Laden von Firmware zu tun haben, in der Datei `/dev/mdev.log` protokolliert.

**DEBUG\_IPTABLES** Standard-Einstellung: `DEBUG_IPTABLES='no'`

Mit `DEBUG_IPTABLES='yes'` werden alle `iptables`-Aufrufe inklusive dem Rückgabewert in `/var/log/iptables.log` protokolliert.

**DEBUG\_IP** Standard-Einstellung: `DEBUG_IP='no'`

Diese Variable aktiviert bei `DEBUG_IP='yes'` das Protokollieren aller Aufrufe des Programms `/sbin/ip` in der Datei `/var/log/wrapper.log`.

## 3.5. Verwendung einer eigenen `/etc/inittab`

Man kann von Init zusätzliche Programme auf zusätzlichen Konsolen starten lassen oder die Standardkommandos der Init-Konfigurationsdatei verändern. Ein Eintrag sieht wie folgt aus:

```
device:runlevel:action:command
```

Das *device* ist das Gerät, über das das Programm seine Ein-/Ausgaben machen soll. Möglich sind hier die normalen Terminals `tty1-tty4` oder serielle Terminals `ttyS0-ttySn` mit  $n < \text{Anzahl}$  der vorhandenen seriellen Schnittstellen.

Als *action* kommen in der Regel *askfirst* oder *respawn* in Frage. Bei *askfirst* wird auf einen Tastendruck gewartet, bevor das Kommando ausgeführt wird, bei *respawn* wird es automatisch neu gestartet, wenn sich das Programm beendet.

*command* ist das Programm, das ausgeführt werden soll. Es ist mit vollständiger Pfadangabe zu spezifizieren.

Die Busybox-Dokumentation unter <http://www.busybox.net> enthält eine genaue Beschreibung des `inittab` Formats.

Die normale `inittab` sieht wie folgt aus:

```
::sysinit:/etc/rc
::respawn:cttyhack /usr/local/bin/mini-login
::ctrlaltdel:/sbin/reboot
::shutdown:/etc/rc0
::restart:/sbin/init
```

Diese könnte man z.B. um den Eintrag

```
tty2::askfirst:cttyhack /usr/local/bin/mini-login
```

erweitern, um ein zweites Login auf Terminal zwei zu bekommen. Dazu einfach die Datei `opt/etc/inittab` nehmen, nach `<config verzeichnis>/etc/inittab` kopieren und mit einem Editor bearbeiten.

## 3.6. Länderspezifische Tastaturlayouts

**KEYBOARD\_LOCALE** Standard-Einstellung: `KEYBOARD_LOCALE='auto'`

Wenn man öfter direkt auf dem fli4l Router arbeitet ist ein lokales Tastaturlayout eine willkommene Hilfe. Mit `KEYBOARD_LOCALE='auto'` wird versucht, ein Tastaturlayout passend zu der Einstellung von `LOCALE` zu benutzen. Mit der Einstellung `"` wird kein lokales Tastaturlayout auf dem fli4l-Router installiert; es wird dann das im Kernel anwesende Standardlayout verwendet. Alternativ kann man auch den Namen einer lokalen Tastaturlayoutmap direkt angeben. Wenn z.B. `'de-latin1'` eingestellt wird, prüft der Buildprozess ob in `opt/etc` eine Datei mit Namen `de-latin1.map` vorliegt. Wenn ja, wird die entsprechende `.map`-Datei als Tastaturlayout eingebunden.

**OPT\_MAKEKBL** Standard-Einstellung: `OPT_MAKEKBL='no'`

Wenn man für seine Tastatur eine map Datei erstellen will muss man wie folgt vorgehen:

- `OPT_MAKEKBL` auf `'yes'` setzen.
- Auf dem Router `'makekbl.sh'` anrufen. Vorzugsweise macht man dies über eine ssh-Verbindung weil das Tastaturlayout sich ändert und das lästig sein kann.
- Die Anweisungen befolgen.
- Ihre neue `<locale>.map` Datei liegt in der `/tmp`.
- Die Arbeiten direkt auf dem Router sind jetzt abgeschlossen.
- Nun kopieren Sie die eben erzeugte Tastaturtabelle in Ihr fli4l-Verzeichnis unter `opt/etc/<locale>.map`. Wenn Sie jetzt `KEYBOARD_LOCALE='<locale>'` setzen wird beim nächsten Buildprozess Ihre neu erzeugtes Tastaturlayout benutzt.
- Vergessen Sie nicht `OPT_MAKEKBL` wieder auf `'no'` zu setzen.

## 3.7. Ethernet-Netzwerkkarten-Treiber

**NET\_DRV\_N** Standard-Einstellung: `NET_DRV_N='1'`

### 3. Basiskonfiguration

Anzahl der benötigten Netzwerkkarten-Treiber.

Wird der Router nur für ISDN verwendet, so gibt es in der Regel nur eine Netzwerkkarte, der Standard-Wert ist also 1.

Bei DSL werden jedoch meistens zwei Netzwerkkarten verwendet.

Hierbei muss man zwei Fälle unterscheiden:

1. Beide Karten sind vom gleichen Typ. Dann muss nur ein Treiber geladen werden, der dann beide Karten anspricht, also `NET_DRV_N='1'`.
2. Es werden zwei verschiedene Karten verwendet, dann muss man hier '2' angeben und den Treiber für die zweite Karte angeben.

**NET\_DRV\_x** Standard-Einstellung: `NET_DRV_1='ne2k-pci'`

Hier wird der Treiber für die Netzwerkkarte angegeben. Über die Variable `NET_DRV_1` wird standardmäßig der Treiber für eine NE2000-kompatible Netzwerkkarte geladen. Weitere verfügbare Treiber für Netzwerkkartenfamilien sind in den Tabellen ?? und ?? eingetragen.

Die 3COM EtherLinkIII (3c509) muss über das Dostool `3c509cfg.exe` (beziehbar von <ftp://ftp.ihg.uni-duisburg.de/Hardware/3com/3C5x9n/3C5X9CFG.EXE>)

konfiguriert werden. Dabei sollten IRQ und I/O-Port und gegebenenfalls auch der Anschluss (BNC/TP) eingestellt werden.

**NET\_DRV\_x\_OPTION** Standard-Einstellung: `NET_DRV_x_OPTION=""`

Der Eintrag kann in der Regel leer bleiben.

Bei manchen ISA-Karten braucht der Treiber zusätzliche Informationen, um die Karte zu finden, z.B. die I/O-Adresse. Bei NE2000-kompatiblen ISA-Karten und bei der EtherExpress16 ist dies zum Beispiel der Fall.

Hier ist z.B.

```
NET_DRV_x_OPTION='io=0x340'
```

zu setzen (oder der entsprechende numerische Wert).

Ist keine Option nötig, kann die Variable leer gelassen werden.

Sind mehrere Optionen nötig, sind diese durch Leerzeichen zu trennen, z.B.

```
NET_DRV_x_OPTION='irq=9 io=0x340'
```

Werden zwei identische Netzwerkkarten verwendet, z.B. NE2000-ISA-Karten, müssen die verschiedenen I/O-Werte durch Komma getrennt werden, also

```
NET_DRV_x_OPTION='io=0x240,0x300'
```

### 3. Basiskonfiguration

Die beiden IO-Werte müssen durch Komma ohne Blank getrennt werden!

Dieses funktioniert nicht bei allen Netzwerkkarten-Treibern. Einige muss man auch doppelt laden, also dann `NET_DRV_N='2'`. In diesem Fall müssen aber mit der Option `"-o"` verschiedene Namen vergeben werden, z.B.

```
NET_DRV_N='2'
NET_DRV_1='3c503'
NET_DRV_1_OPTION='-o 3c503-0 io=0x280'
NET_DRV_2='3c503'
NET_DRV_2_OPTION='-o 3c503-1 io=0x300'
```

Unser Tip: erst die Komma-Methode ausprobieren, danach das mehrfache Laden mit Option `"-o"` versuchen.

Nachfolgend noch einige Beispiele von Netzwerkkarten:

- 1 x NE2000 ISA

```
NET_DRV_1='ne'
NET_DRV_1_OPTION='io=0x340'
```

- 1 x 3COM EtherLinkIII (3c509)

```
NET_DRV_1='3c509'
NET_DRV_1_OPTION=''
```

Siehe zu dieser Karte auch:

[http://extern.fli4l.de/fli4l\\_faengine/faq.php?display=faq&faqnr=132&catnr=7&prog=1](http://extern.fli4l.de/fli4l_faengine/faq.php?display=faq&faqnr=132&catnr=7&prog=1)

[http://extern.fli4l.de/fli4l\\_faengine/faq.php?display=faq&faqnr=133&catnr=7&prog=1](http://extern.fli4l.de/fli4l_faengine/faq.php?display=faq&faqnr=133&catnr=7&prog=1)

[http://extern.fli4l.de/fli4l\\_faengine/faq.php?display=faq&faqnr=135&catnr=7&prog=1](http://extern.fli4l.de/fli4l_faengine/faq.php?display=faq&faqnr=135&catnr=7&prog=1)

- 2 x NE2000 ISA

```
NET_DRV_1='ne'
NET_DRV_1_OPTION='io=0x320,0x340'
```

Oft muss man hier noch die IRQ-Werte mit angeben, also

```
NET_DRV_1_OPTION='io=0x320,0x340 irq=3,5'
```

Man sollte es hier zunächst ohne Angabe der Interrupts probieren und lediglich dann die Interrupts eintragen, wenn ohne Angabe der Interrupts die Netzwerkkarten nicht gefunden werden.

- 2 x NE2000 PCI

```
NET_DRV_1='ne2k-pci'
NET_DRV_1_OPTION=''
```



- 1 x NE2000 ISA, 1 x NE2000 PCI

```
NET_DRV_1='ne'  
NET_DRV_1_OPTION='io=0x340'  
NET_DRV_2='ne2k-pci'  
NET_DRV_2_OPTION=''
```

- 1 x SMC WD8013, 1 x NE2000 ISA

```
NET_DRV_1='wd'  
NET_DRV_1_OPTION='io=0x270'  
NET_DRV_2='ne2k'  
NET_DRV_2_OPTION='io=0x240'
```

Die vollständige Liste der verfügbaren Treiber finden Sie in der Dokumentation des jeweiligen Kernel-Pakets.

Falls Sie ein dummy-Device brauchen, verwenden Sie 'dummy' für `NET_DRV_x` und `IP_NET_x_DEV` (Seite 42)='dummy<Nummer>' als Device-Name.

## 3.8. Netzwerk-Konfiguration (IPv4)

**OPT\_IPV4** Aktiviert die IPv4-Unterstützung.

**Wichtig:** Diese Einstellung muss zur Zeit den Wert 'yes' beinhalten! Ein reiner IPv6-Betrieb ist zur Zeit noch nicht möglich!

Standard-Einstellung: `OPT_IPV4='yes'`

**IP\_NET\_N** Standardwert: `IP_NET_N='1'`

Anzahl der Netzwerke, die an das IPv4-Protokoll gebunden werden sollen. Im Normalfall also '1'. Falls es keine Netzwerke geben sollte oder sie über einen anderen Weg konfiguriert werden, und daher `IP_NET_N` auf 0 gesetzt wird, wird beim Bauen der Archive eine Warnung ausgegeben. Diese kann man durch setzen von `IGNOREIPNETWARNING='yes'` ausschalten.

**IP\_NET\_x** Standardwert: `IP_NET_1='192.168.6.1/24'`

Die IPv4-Adresse und die Netzmaske in CIDR<sup>1</sup>-Schreibweise des x'ten Devices im fli4l-Router. Wird die IPv4-Adresse dynamisch durch einen DHCP-Klienten zugewiesen, kann hier auch 'dhcp' als Wert eingetragen werden.

Nachfolgende Tabelle zeigt CIDR und Punkt-Schreibweise (DOT Notation).

---

<sup>1</sup>Classless Inter-Domain Routing

### 3. Basiskonfiguration

CIDR	Netzmaske	Anzahl IPs
/8	255.0.0.0	16777216
/16	255.255.0.0	65536
/23	255.255.254.0	512
/24	255.255.255.0	256
/25	255.255.255.128	128
/26	255.255.255.192	64
/27	255.255.255.224	32
/28	255.255.255.240	16
/29	255.255.255.248	8
/30	255.255.255.252	4
/31	255.255.255.254	2
/32	255.255.255.255	1

**Anmerkung:** Da jeweils eine IPv4 für die Netzwerk- und Broadcast-Adresse reserviert sind, errechnet sich die maximale Anzahl der Hosts im Netzwerk zu: `Anzahl_Hosts = Anzahl_IPs - 2`. Die kleinste mögliche Netzmaske wäre also /30, entspricht 4 IPs und somit 2 möglichen Hosts.

**IP\_NET\_x\_DEV** Standard-Einstellung: `IP_NET_1_DEV='eth0'`

Erforderlich: Device-Name der Netzwerkkarte.

Ab Version 2.1.8 ist die Angabe des verwendeten Device zwingend erforderlich! Die Namen der Devices beginnen in den meisten Fällen mit `'eth'` gefolgt von einer Zahl. Die erste vom System erkannte Netzwerkkarte bekommt den Namen `'eth0'`, die zweite `'eth1'` usw.

Beispiel:

```
IP_NET_1_DEV='eth0'
```

fl4l beherrscht auch IP-Aliasing, also die Zuweisung von mehreren IPs auf eine Netzwerkkarte. Zusätzliche IPs definiert man einfach mit einem weiteren Netzwerk auf dem selben Device. Beim Überprüfen der Konfiguration informiert mkfl4l darüber, dass man ein solches Alias definiert — diese Warnung kann man dann ignorieren.

Beispiel:

```
IP_NET_1='192.168.6.1/24'
IP_NET_1_DEV='eth0'
IP_NET_2='192.168.7.1/24'
IP_NET_2_DEV='eth0'
```

**IP\_NET\_x\_MAC** Standard-Einstellung: `IP_NET_1_MAC=""`

Optional: MAC-Adresse der Netzwerkkarte.

### 3. Basiskonfiguration

Hier kann die Hardwareadresse (MAC) der Netzwerkkarte angepasst werden. Dies ist zum Beispiel nützlich, wenn Sie einen DHCP-Provider nutzen wollen, der eine bestimmte MAC-Adresse erwartet. Wird `IP_NET_x_MAC` leer gelassen oder gar nicht angegeben, so wird die voreingestellte MAC-Adresse der Netzwerkkarte verwendet. Die allermeisten Nutzer werden diese Variable nicht benötigen.

Beispiel:

```
IP_NET_1_MAC='01:81:42:C2:C3:10'
```

**IP\_NET\_x\_NAME** Standard-Einstellung: `IP_NET_x_NAME=""`

Optional: Der IPv4-Adresse der Netzwerkkarte einen Namen geben.

Bei umgekehrter Namensauflösung der IPv4-Adresse der Netzwerkkarte erscheint standardmässig ein Name der Form `'fli4l-ethx.<domain>'`. In `IP_NET_x_NAME` kann man selbst einen anderen Namen angeben. Dieser Name wird dann bei umgekehrter Namensauflösung angezeigt. Bei einer öffentlichen IPv4-Adresse kann man so erreichen, dass immer der öffentliche Name aufgelöst wird.

Beispiel:

```
IP_NET_2='80.126.238.229/32'
IP_NET_2_NAME='ajv.xs4all.nl'
```

**IP\_NET\_x\_TYPE**

**IP\_NET\_x\_COMMENT** Standard-Einstellung: `IP_NET_x_COMMENT=""`

Optional: Die Angabe dient dazu, einem Device einen 'aussagekräftigen' Namen zu geben. Dieser kann dann in Paketen wie z.B. `rrdtool` zur Identifikation des Netzwerks verwendet werden.

## 3.9. Netzwerk-Konfiguration (IPv6)

### 3.9.1. Einleitung

Zusätzlich zu der im letzten Abschnitt vorgestellten Konfiguration von IPv4-Netzwerken ist es auch möglich, den fli4l-Router in vielerlei Hinsicht IPv6-tauglich zu machen. Dazu gehören Angaben über die IPv6-Adresse des Routers, die verwalteten IPv6-(Sub-)Netze sowie vordefinierte IPv6-Routen und Firewall-Regeln bzgl. IPv6-Paketen. IPv6 ist der Nachfolger des Internet-Protokolls IPv4. Hauptsächlich wurde es entwickelt, um die relativ kleine Menge von eindeutigen Internet-Adressen zu vergrößern: Während IPv4 ungefähr  $2^{32}$  Adressen unterstützt,<sup>2</sup> sind es bei IPv6 bereits  $2^{128}$  Adressen. Dadurch kann mit IPv6 jedem kommunizierenden Host eine eindeutige Adresse zugeordnet werden, und man ist nicht mehr auf Techniken wie NAT, PAT, Masquerading etc. angewiesen.

---

<sup>2</sup>nur ungefähr, weil einige Adressen speziellen Zwecken dienen, etwa für Broad- und Multicasting

Neben diesem Aspekt spielten bei der Entwicklung des IPv6-Protokolls auch Themen wie Selbstkonfiguration und Sicherheit eine Rolle. Dies wird in späteren Abschnitten aufgegriffen.

Das größte Problem bei IPv6 ist dessen Verbreitung: Momentan wird IPv6 – verglichen mit IPv4 – nur sehr spärlich verwendet. Das liegt daran, dass IPv6 und IPv4 technisch nicht miteinander kompatibel sind und somit alle Software- und Hardware-Komponenten, die an der Paket-Weiterleitung im Internet beteiligt sind, für IPv6 nachgerüstet werden müssen. Auch bestimmte Dienste wie DNS (Domain Name System) müssen für IPv6 entsprechend aufgeböhrt werden.

Hier tut sich also ein Teufelskreis auf: Die geringe Verbreitung von IPv6 bei Diensteanbietern im Internet führt zu Desinteresse seitens der Router-Hersteller, ihre Geräte mit IPv6-Funktionalität auszustatten, was wiederum dazu führt, dass Dienstanbieter die Umstellung auf IPv6 scheuen, weil sie fürchten, dass sich der Aufwand nicht lohnt. Erst langsam wendet sich das Blatt zugunsten von IPv6, nicht zuletzt unter dem immer stärkeren Druck der knappen Adressvorräte.<sup>3</sup>

#### 3.9.2. Adressformat

Eine IPv6-Adresse besteht aus acht Zwei-Byte-Werten, die hexadezimal notiert werden:

*Beispiel 1:* 2001:db8:900:551:0:0:0:2

*Beispiel 2:* 0:0:0:0:0:0:0:1 (IPv6-Loopback-Adresse)

Um die Adressen etwas übersichtlicher zu gestalten, werden aufeinander folgende Nullen zusammengelegt, indem sie entfernt werden und lediglich zwei unmittelbar aufeinander folgende Doppelpunkte verbleiben. Die obigen Adressen können also auch so geschrieben werden:

*Beispiel 1 (kompakt):* 2001:db8:900:551::2

*Beispiel 2 (kompakt):* ::1

Eine solche Kürzung ist aber nur höchstens einmal erlaubt, um Mehrdeutigkeiten zu vermeiden. Die Adresse 2001:0:0:1:2:0:0:3 kann also entweder zu 2001::1:2:0:0:3 oder zu 2001:0:0:1:2::3 verkürzt werden, nicht aber zu 2001::1:2::3, da jetzt unklar wäre, wie die vier Nullen jeweils auf die zusammengezogenen Bereiche verteilt werden sollen.

Eine weitere Mehrdeutigkeit existiert, wenn eine IPv6-Adresse mit einem Port (TCP oder UDP) kombiniert werden soll: In diesem Fall darf man den Port nicht unmittelbar mit Doppelpunkt und Wert anschließen, weil der Doppelpunkt bereits innerhalb der Adresse verwendet wird und somit in manchen Fällen unklar wäre, ob die Port-Angabe nicht vielleicht doch eine Adress-Komponente darstellt. Deshalb muss in solchen Fällen die IPv6-Adresse in eckigen Klammern angegeben werden. Dies ist auch die Syntax, wie sie in URLs gefordert wird (etwa wenn im Web-Browser eine numerische IPv6-Adresse verwendet werden soll).

*Beispiel 3:* [2001:db8:900:551::2]:1234

Ohne die Verwendung von Klammern entsteht die Adresse 2001:db8:900:551::2:1234, die unverkürzt der Adresse 2001:db8:900:551:0:0:2:1234 entspricht und somit keine Port-Angabe besitzt.

Wenn Sie keinen Internet-Zugang mit nativer IPv6-Anbindung nutzen können, benötigen Sie einen IPv6-Tunnel zu einem IPv6-Anbieter. Dies wird durch das Paket “ipv6” ermöglicht. Bitte lesen Sie die Dokumentation des “ipv6”-Pakets für Details.

---

<sup>3</sup>Inzwischen sind die letzten IPv4-Adressblöcke von der IANA vergeben worden.

#### 3.9.3. Konfiguration

##### Allgemeine Einstellungen

Die allgemeinen Einstellungen beinhalten zum einen die Aktivierung der IPv6-Unterstützung und zum anderen die optionale Vergabe einer IPv6-Adresse an den Router.

**OPT\_IPV6** Aktiviert die IPv6-Unterstützung.

Standard-Einstellung: `OPT_IPV6='no'`

**HOSTNAME\_IP6** (optional) Diese Variable stellt explizit die IPv6-Adresse des Routers ein. Falls die Variable nicht gesetzt wird, wird die IPv6-Adresse auf die Adresse des ersten konfigurierten IPv6-Subnetzes gesetzt (`IPV6_NET_x`, siehe unten).

Beispiel: `HOSTNAME_IP6='IPV6_NET_1_IPADDR'`

##### Subnetz-Konfiguration

In diesem Abschnitt wird die Konfiguration von einem oder mehreren IPv6-Subnetzen vorgestellt. Ein IPv6-Subnetz ist ein IPv6-Adressraum, der über ein so genanntes Präfix spezifiziert wird und an eine bestimmte Netzwerk-Schnittstelle gebunden ist. Weitere Einstellungen betreffen das Veröffentlichen des Präfixes und des DNS-Dienstes innerhalb des Subnetzes sowie einen optionalen Router-Namen innerhalb dieses Subnetzes.

**IPV6\_NET\_N** Diese Variable enthält die Anzahl der verwendeten IPv6-Subnetze. Mindestens ein IPv6-Subnetz sollte definiert werden, um IPv6 im lokalen Netz nutzen zu können.

Standard-Einstellung: `IPV6_NET_N='0'`

**IPV6\_NET\_x** Diese Variable enthält für ein bestimmtes IPv6-Subnetz die IPv6-Adresse des Routers sowie die Größe der Netzmaske in CIDR-Notation. Soll das Subnetz öffentlich geroutet werden, so stammt es in der Regel vom Internet- bzw. Tunnel-Anbieter.

**Wichtig:** *Soll in dem Subnetz die zustandslose Selbstkonfiguration (siehe den Abschnitt zu `IPV6_NET_x_ADVERTISE` weiter unten) aktiviert werden, dann muss die Länge des Subnetz-Präfixes 64 Bit betragen!*

Ist das Subnetz an einen Tunnel angeschlossen oder wird DHCPv6 zum Ermitteln eines Präfixes verwendet, dann darf hier nur der Teil der Router-Adresse angegeben werden, der *nicht* zum dem Tunnel zugeordneten bzw. vom DHCPv6-Server erhaltenen Subnetz-Präfixes gehört, da jenes Präfix und diese Adresse miteinander kombiniert werden! Siehe die Dokumentation der “`ipv6`”- (Tunnel) bzw. “`dns_dhcp`”-Pakete (DHCPv6) für Details.

Beispiele:

<code>IPV6_NET_1='2001:db8:1743:42::1/64'</code>	# statisch: komplette Adresse
<code>IPV6_NET_2='{he}+0:0:0:42::1/64'</code>	# HE-Tunnel: partielle Adresse
<code>IPV6_NET_3='{dhcpv6}+0:0:0:43::1/64'</code>	# DHCPv6: partielle Adresse

**IPV6\_NET\_x\_DEV** Diese Variable enthält für ein bestimmtes IPv6-Subnetz den Namen der Netzwerk-Schnittstelle, an welche das IPv6-Netz gebunden wird. Dies kollidiert *nicht* mit den in der Basis-Konfiguration (`base.txt`) vergebenen Netzwerk-Schnittstellen, da einer Netzwerk-Schnittstelle sowohl IPv4- als auch IPv6-Adressen zugeordnet werden dürfen.

Beispiel: `IPV6_NET_1_DEV='eth0'`

**IPV6\_NET\_x\_ADVERTISE** Diese Variable legt fest, ob das eingestellte Subnetz-Präfix im LAN mittels “Router Advertisements” verbreitet wird. Dies wird für die so genannte “stateless autoconfiguration” (zustandslose Selbstkonfiguration) verwendet und ist nicht mit DHCPv6 zu verwechseln. Mögliche Werte sind “yes” und “no”.

Es ist empfehlenswert, diese Einstellung zu aktivieren, es sei denn, alle Adressen im Netz werden statisch vergeben oder ein anderer Router ist bereits dafür zuständig, das Subnetz-Präfix anzukündigen.

**Wichtig:** *Die automatische Verteilung des Subnetzes funktioniert nur, wenn das Subnetz ein /64-Netz ist, d.h. wenn die Länge des Subnetz-Präfixes 64 Bit beträgt! Der Grund hierfür ist, dass die anderen Hosts im Netzwerk ihre IPv6-Adresse aus dem Präfix und ihrer Host-MAC-Adresse berechnen und dies nicht funktioniert, wenn der Host-Anteil nicht 64 Bit beträgt. Wenn die Selbstkonfiguration fehlschlägt, sollte also geprüft werden, ob das Subnetz-Präfix nicht vielleicht falsch angegeben worden ist (z.B. als /48).*

Standard-Einstellung: `IPV6_NET_1_ADVERTISE='yes'`

**IPV6\_NET\_x\_ADVERTISE\_DNS** Diese Variable legt fest, ob auch der lokale DNS-Dienst im IPv6-Subnetz mittels “Router Advertisements” (RDNSS-Option) angekündigt werden soll. Dies funktioniert aber nur, wenn die IPv6-Funktionalität des DNS-Dienstes mit Hilfe der Variable `DNS_SUPPORT_IPV6='yes'` aktiviert ist. Mögliche Werte sind “yes” und “no”.

Standard-Einstellung: `IPV6_NET_1_ADVERTISE_DNS='no'`

**IPV6\_NET\_x\_NAME** (optional) Diese Variable legt einen Interface-spezifischen Hostnamen für den Router in diesem IPv6-Subnetz fest.

Beispiel: `IPV6_NET_1_NAME='fli4l-subnet1'`

## 3.10. Netzwerkpräfix-Konfiguration

**OPT\_NET\_PREFIX** Aktiviert die Unterstützung für selbstdefinierte Netzwerkpräfixe.

Ein Netzwerkpräfix ist technisch nichts anderes als die Adresse eines Netzwerks, allerdings steht es i. d. R. für ein Netz, das weiter unterteilt werden soll. Sinnvoll ist dies vor allem dann, wenn ein fli4l-Router ein Netzwerk nicht alleine verwaltet, sondern Teilnetze daraus anderen Routern zur Verwaltung überlässt. Durch die Definition und somit die Benennung des insgesamt zur Verfügung und Verteilung stehenden Netzes ist es möglich, die Netzwerk-Adresse an mehreren Stellen zu verwenden, ohne den gemeinsamen Präfix immer wieder hinschreiben zu müssen.

Konkrete Beispiele, wie man ein Netzwerkpräfix definiert, sind weiter unten bei den verschiedenen Typen von Netzwerkpräfixen zu finden.

Standard-Einstellung: `OPT_NET_PREFIX='yes'`

**NET\_PREFIX\_x** Über dieses Array werden die verschiedenen Netzwerkpräfixe definiert. Die einzelnen Komponenten werden im Anschluss erklärt.

**NET\_PREFIX\_x\_NAME** Name des Netzwerkpräfixes.

Diese Variable enthält den Namen des Präfixes. Dieser Name kann dann in Adressangaben verwendet werden, um das Präfix zu benutzen. Dabei wird der Name analog zu Circuit-Namen verwendet, d. h. er muss in geschweiften Klammern geschrieben werden.

**NET\_PREFIX\_x\_TYPE** Typ des Netzwerkpräfixes.

Diese Variable enthält den Typ des Präfixes. Die unterstützten Typen werden in Tab. 3.3 erläutert.

Typ	Bedeutung
static	Das Netzwerkpräfix wird direkt als feste Adresse angegeben.
generated-ula	Das Netzwerkpräfix ist eine vom fli4l generierte ULA <sup>4</sup> gemäß RFC 4193. <sup>5</sup> Wenn der fli4l Zugriff auf persistenten Speicher hat, dann wird das Präfix nur einmal generiert, so dass es auch über Neustarts des Routers hinweg stabil bleibt.

Tabelle 3.3.: Typen von Netzwerkpräfixen

#### 3.10.1. Netzwerkpräfixe vom Typ “stable”

Für Netzwerkpräfixe vom Typ “stable” gibt es die folgenden Einstellungen:

**NET\_PREFIX\_x\_STATIC\_IPV4 NET\_PREFIX\_x\_STATIC\_IPV6** Adresse(n) des Netzwerkpräfixes.

Mit Hilfe dieser Einstellung kann die IPv4- und/oder die IPv6-Adresse des Netzwerkpräfixes angegeben werden.

Beispiel:

```
NET {
  PREFIX {
    [] {
      NAME='site'
      TYPE='static'
      STATIC {
        IPV4='10.1.0.0/16'
        IPV6='fdce:1c35:301f::/48'
      }
    }
  }
}
```

<sup>4</sup>“Unique Local Address”

<sup>5</sup><https://tools.ietf.org/html/rfc4193>

### 3.10.2. Netzwerkpräfixe vom Typ “generated-ula”

Für Netzwerkpräfixe vom Typ “generated-ula” gibt es die folgenden Einstellungen:

**NET\_PREFIX\_x\_ULA\_DEV** Ethernet-Schnittstelle.

Mit Hilfe dieser Einstellung wird die Ethernet-Schnittstelle angegeben, deren MAC-Adresse für die Generierung der ULA herangezogen wird.

Beispiel:

```
NET {
  PREFIX {
    [] {
      NAME='site'
      TYPE='generated-ula'
      ULA {
        DEV='eth0'
      }
    }
  }
}
```

## 3.11. Zusätzliche Routen (IPv4)

**IP\_ROUTE\_N** Standard-Einstellung: `IP_ROUTE_N='0'`

Anzahl von zusätzlichen Netzwerkrouuten. Zusätzliche Netzwerkrouuten sind zum Beispiel dann erforderlich, wenn sich im LAN weitere Router befinden, über die andere Netzwerke erreichbar sein sollen.

Im Normalfall ist die Angabe von weiteren Netzwerkrouuten nicht erforderlich.

**IP\_ROUTE\_x** Die zusätzlichen Routen `IP_ROUTE_1`, `IP_ROUTE_2`, ... haben folgenden Aufbau:

```
network/netmaskbits gateway
```

Dabei ist **network** die Netzwerkadresse, **/netmaskbits** die Netzmaske in [CIDR](#) (Seite 42) Schreibweise und **gateway** die Adresse des Rechners, der die Verbindung zu dem Netzwerk herstellt. Der Gateway-Rechner muss natürlich im gleichen Netzwerk, wie der fli4l-Router liegen! Ist z.B. das Netzwerk 192.168.7.0 mit der Netzwerkmaske 255.255.255.0 über das Gateway 192.168.6.99 erreichbar, dann lautet der Eintrag:

```
IP_ROUTE_N='1'
IP_ROUTE_1='192.168.7.0/24 192.168.6.99'
```

Wenn der fli4l-Router nicht als Internet-Router eingesetzt wird sondern nur als reiner Ethernetrouter kann man in einem `IP_ROUTE_x` Eintrag eine Default-Route angeben. Dazu wird analog zu der `network/netmaskbits` Schreibweise `0.0.0.0/0` eingetragen, so wie im Beispiel zu sehen ist.



```
IP_ROUTE_N='3'  
IP_ROUTE_1='192.168.1.0/24 192.168.6.1'  
IP_ROUTE_2='10.73.0.0/16 192.168.6.1'  
IP_ROUTE_3='0.0.0.0/0 192.168.6.99'
```

Intern werden die hierüber spezifizierten Routen in Circuits (siehe [Circuits vom Typ “route”](#) (Seite 103)) umgewandelt. Dabei werden alle Routen mit demselben Gateway demselben Circuit zugeordnet.

## 3.12. Zusätzliche Routen (IPv6)

IPv6-Routen sind Wege für IPv6-Pakete. Damit der Router weiß, welches eingehende Paket er wohin schicken soll, greift er auf eine Routing-Tabelle zurück, in der genau diese Informationen zu finden sind. Im Falle von IPv6 ist es wichtig zu wissen, wohin IPv6-Pakete geschickt werden, die nicht ins lokale Netz sollen.

**IPV6\_ROUTE\_N** Diese Variable legt die Anzahl der zu spezifizierenden IPv6-Routen fest. In der Regel werden keine zusätzlichen IPv6-Routen benötigt.

Standard-Einstellung: `IPV6_ROUTE_N='0'`

**IPV6\_ROUTE\_x** Diese Variable enthält die Route in der Form ‘Zielnetz Gateway’, wobei das Zielnetz in der CIDR-Notation erwartet wird. Für die Default-Route muss als Zielnetz `::/0` verwendet werden.

Beispiel: `IPV6_ROUTE_1='2001:db8:1743:44::/64_2001:db8:1743:44::1'`

## 3.13. Der Paketfilter (IPv4)

Der von fli4l verwendete Linux-Kern stellt einen Paketfilter zur Verfügung. Mit Hilfe dieses Paketfilters wird gesteuert, wer mit dem Router bzw. über ihn hinweg kommunizieren darf. Weiterhin können Dinge wie Port-Weiterleitung (ein an den Router gerichtetes Paket wird an einen anderen internen Rechner weitergereicht) und Maskierung (engl. “Masquerading”; Pakete, die von einem Rechner hinter dem Router kommen, werden so verändert, dass sie so aussehen, als kämen sie vom Router selbst) realisiert werden.

Die Struktur des Paketfilters ist in Abbildung 3.1 angedeutet. Pakete kommen über eine Netzwerk-Schnittstelle herein und durchlaufen die `PREROUTING`-Kette (eng. “chain”). Hier werden die an den Router gerichteten Pakete an einen anderen Rechner weitergereicht, indem die Zieladresse und der Zielport manipuliert werden. Ist das Paket an den Router gerichtet, wird es an die `INPUT`-Kette, andernfalls an die `FORWARD`-Kette weitergereicht. Beide Ketten prüfen, ob das Paket zulässig ist. Wird das Paket akzeptiert, wird es an den lokalen Zielprozess zugestellt oder über die `POSTROUTING`-Kette (in der das Maskieren von Paketen stattfindet) an diejenige Netzwerk-Schnittstelle weitergereicht, über die das Paket sein Ziel erreichen kann. Lokal generierte Pakete werden in der `OUTPUT`-Kette gefiltert und schließlich (falls erfolgreich) über die `POSTROUTING`-Kette ebenfalls an die korrekte Netzwerk-Schnittstelle weitergereicht.

Mit der Paketfilterkonfiguration lassen sich die einzelnen Ketten des Paketfilters direkt konfigurieren. Dazu gibt es für jede relevante Kette ein eigenes Array, d.h. eine für die `INPUT`-Kette (`PF_INPUT_%`), eine für die `FORWARD`-Kette (`PF_FORWARD_%`), eine für die `OUTPUT`-Kette

### 3. Basiskonfiguration



Abbildung 3.1.: Struktur des Paketfilters

(PF\_OUTPUT\_%), eine für die PREROUTING-Kette, in der die Portweiterleitung durchgeführt wird (PF\_PREROUTING\_%), und eine für die POSTROUTING-Kette, in der das Maskieren der Pakete durchgeführt wird (PF\_POSTROUTING\_%).

Ein Eintrag in einem dieser Arrays besteht im Wesentlichen aus einer Aktion (s.u.), die durch zusätzliche Bedingungen eingeschränkt werden kann. Diese Bedingungen beziehen sich auf Eigenschaften des betrachteten Paketes. Ein Paket enthält Informationen über seine Herkunft (Quelle, welcher Rechner hat das Paket losgeschickt), sein Ziel (an welchen Rechner und welche Anwendung soll das Paket gehen) u.a.m. Bedingungen können sich auf folgende Eigenschaften eines Paketes beziehen:

- die Quelle (Quell-Adresse, Quell-Port oder beides)
- das Ziel (Ziel-Adresse, Ziel-Port oder beides)
- das Protokoll
- die Schnittstelle, über welches das Paket hereinkommt bzw. hinausgeht
- die MAC-Adresse des Rechners, von dem das Paket kommt
- den Zustand des Paketes bzw. der Verbindung, zu der das Paket gehört

Kommt ein Paket herein, werden die Einträge bzw. die daraus generierten Regeln von oben nach unten abgearbeitet und die erste Aktion ausgeführt, bei der alle Bedingungen gelten. Trifft keine der Regeln zu, wird die Standardaktion ausgeführt, die man für (fast) jede Tabelle angeben kann.

Ein Eintrag hat dabei folgendes Format, wobei zu beachten ist, dass alle Einschränkungen optional sind:

```
restriction{0,} [[source] [destination]] action [BIDIRECTIONAL|LOG|NOLOG]
```

An allen Stellen, an denen Netzwerke, IP-Adressen oder Hosts angegeben werden müssen, kann man sich auch auf IP\_NET\_%, IP\_NET\_%\_IPADDR oder via @hostname auf einen Host aus HOST\_% beziehen. Ist OPT\_DNS aktiviert, dann können außerhalb von Aktionen via @fqdn auch Hosts über ihren Namen referenziert werden, die *nicht* in HOST\_% zu finden sind. Das ist insbesondere dann sinnvoll, wenn es sich um externe Hosts handelt, die zudem viele (und wechselnde) IP-Adressen besitzen.

## 3.13.1. Aktionen des Paketfilters

Aktionen können die folgenden sein:

Aktion	Kette(n)	Bedeutung
ACCEPT	alle	Akzeptiere das Paket.
DROP	INPUT FORWARD OUTPUT	Verwirf das Paket (der Absender erkennt das nur daran, dass keine Antwort, aber auch keine Fehlermeldung zurückkommt).
REJECT	INPUT FORWARD OUTPUT	Weise das Paket zurück (der Absender erhält eine entsprechende Fehlermeldung).
LOG	alle	Protokolliere das Paket und gehe zur nächsten Regel. Um verschiedene Protokoll-Einträge auseinanderhalten zu können, kann ein Präfix verwendet werden, das via LOG:log-prefix angegeben wird. Dieses Präfix darf maximal 28 Zeichen lang sein und kann aus Buchstaben, Ziffern, dem Bindestrich (-) und dem Unterstrich (_) bestehen.
MASQUERADE	POSTROUTING	Maskiere das Paket: Ersetze die Quelladresse des Paketes durch die eigene, der Schnittstelle zugewiesenen Adresse und Sorge dafür, dass Antworten für diese Verbindung an den richtigen Rechner weitergeleitet werden.
SNAT	POSTROUTING	Ersetze die Quelladresse und den Quellport des Paketes durch die als Parameter für SNAT angegebene Adresse (für alle Pakete, die zu der gerade betrachteten Verbindung gehören).
DNAT	PREROUTING	Ersetze die Zieladresse und den Zielport des Paketes durch die als Parameter für DNAT angegebene Adresse (für alle Pakete, die zu der gerade betrachteten Verbindung gehören).
REDIRECT	PREROUTING OUTPUT	Ersetze den Zielport des Paketes durch den als Parameter für REDIRECT angegebenen Port und stelle das Paket lokal zu (für alle Pakete, die zu der gerade betrachteten Verbindung gehören).
NETMAP	PREROUTING POSTROUTING	Bilde die Ziel- bzw. Quelladresse des Paketes in den als Parameter für NETMAP angegebenen Bereich ab, die Ports bleiben unverändert (für alle Pakete, die zu der gerade betrachteten Verbindung gehören; in der PREROUTING-Kette wird die Zieladresse verändert, in der POSTROUTING-Kette die Quelladresse).

Tabelle 3.4.: Aktionen in Paketfilterregeln

Einige dieser Aktionen können durch die Optionen `BIDIRECTIONAL`, `LOG` oder `NOLOG` in ihrem Verhalten modifiziert werden. `BIDIRECTIONAL` generiert die gleiche Regel noch einmal, nur mit vertauschter Quell- und Zieladresse (und vertauschtem Quell- und Zielpport und/oder vertauschter ein- und ausgehender Netzwerk-Schnittstelle, falls angegeben). `LOG`/`NOLOG` aktivieren bzw. deaktivieren das Protokollieren für diese eine Regel.

### 3.13.2. Einschränkungen in den Regeln

Einschränkungen können durch die in den folgenden Abschnitten aufgeführten Bedingungen vorgenommen werden. Bei den Bedingungen kann man immer **any** angeben, wenn man an irgendeiner Stelle keine Einschränkung vornehmen will, aber trotzdem etwas angeben will/muss. Einschränkungen können in beliebiger Reihenfolge angegeben werden, wenn sie einen vorangestellten Präfix haben. Das gilt für alle Einschränkungen, außer für die Angabe einer Quell- bzw. Zieladresse. Diese müssen immer direkt vor der Aktion stehen, die anderen Einschränkungen müssen vorher erfolgen. Einschränkungen können auch negiert werden, dazu wird einfach ein **!** vorangestellt.

#### Einschränkungen der Quelle und des Ziels

Jedes Paket enthält eine Quell- und eine Zielangabe, jeweils in Form eines Tupels einer IP-Adresse und eines Ports.<sup>6</sup> Diese Quelle bzw. dieses Ziel kann für eine Einschränkung herangezogen werden. Die Angabe für die Quelle bzw. das Ziel kann folgendermaßen vorgenommen werden:

Ausdruck	Bedeutung
<code>ip</code>	eine einfache IP-Adresse
<code>network</code>	eine Netzwerkangabe der Form <code>&lt;ip&gt;/&lt;netmask&gt;</code>
<code>port[-port]</code>	ein Port bzw. ein Port-Bereich
<code>IP_NET_x_IPADDR</code>	die IP-Adresse der Schnittstelle <code>x</code> des Routers
<code>IP_NET_x</code>	das Subnetz <code>x</code> des Routers
<code>IP_ROUTE_x</code>	das in der Route <code>x</code> angegebene Subnetz (Default-Routen können nicht verwendet werden, sie würden <b>any</b> entsprechen und werden vorsichtshalber ausgeklammert)
<code>@name</code>	einer der via <code>HOST_%*</code> vergebenen Namen oder Aliase; es wird die zugehörige IP-Adresse an dieser Stelle eingesetzt
<code>&lt;ip oder network&gt;:port[-port]</code>	Host- bzw. Netzwerk-Adresse in einer der obigen Varianten, kombiniert mit einem Port bzw. Port-Bereich

Tabelle 3.5.: Quell- und Zieleinschränkungen in Paketfilterregeln

<sup>6</sup>Ein Port ist nur bei TCP- und UDP-Paketen vorhanden.

### 3. Basiskonfiguration

Das könnte z. B. wie folgt aussehen: `'192.168.6.2 any DROP'`

Tauchen zwei dieser Angaben auf, wird die erste als Quelle, die zweite als Ziel betrachtet. In diesem Beispiel verwerfen wir also Pakete, die vom Rechner mit der IP-Adresse 192.168.6.2 gesendet wurden, unabhängig davon, an welches Ziel sie gerichtet sind.

Taucht nur eine Angabe auf, wird anhand des Wertes entschieden, ob die Quelle oder das Ziel gemeint ist, wobei die Entscheidung relativ einfach ist:

- Ist eine Port-Angabe enthalten, ist das Ziel gemeint.
- Sonst ist die Quelle gemeint.

Wenn wir also z. B. das obige Beispiel abkürzen wollten, könnten wir einfach `'192.168.6.2 DROP'` schreiben. Es ist kein Port angegeben, die Bedingung gilt also für die Quelle, den Rechner, von dem das Paket gesendet wurde.

Wollen wir die Kommunikation mit dem `ssh`-Dämon erlauben, können wir `'any any:22 ACCEPT'` (Pakete von einem beliebigen Rechner an den `ssh`-Port 22 eines beliebigen Rechners werden akzeptiert) oder kürzer `'22 ACCEPT'` schreiben: Es ist nur ein Port angegeben, also meinen wir das Ziel und damit Pakete, die an den Port 22 gerichtet sind.

Zur Vereinfachung der Regelmenge kann man an die Aktion ein `BIDIRECTIONAL` dranhängen, um auszudrücken, dass die Regel für beide Kommunikationsrichtungen gilt. Es werden dann Regeln generiert, in denen einfach die Quell- und die Ziel-Adressen und eventuell angegebenen Ports und Netzwerk-Schnittstellen vertauscht sind und der Rest gleich bleibt.

Beispiele:

<code>127.0.0.1 ACCEPT</code>	Lokale Kommunikation (Quelle 127.0.0.1) ist erlaubt
<code>any 192.168.12.1 DROP</code>	Pakete an die Adresse 192.168.12.1 werden weggeworfen
<code>any 192.168.12.1 DROP LOG</code>	Pakete an die Adresse 192.168.12.1 werden weggeworfen und zusätzlich protokolliert
<code>any 192.168.12.1 DROP NOLOG</code>	Pakete an die Adresse 192.168.12.1 werden weggeworfen, werden aber nicht protokolliert
<code>22 ACCEPT</code>	Pakete an den Port 22 ( <code>ssh</code> ) werden akzeptiert
<code>IP_NET_1_NET ACCEPT</code>	Pakete aus dem an der ersten Schnittstelle hängenden Subnetz werden akzeptiert
<code>IP_NET_1_NET IP_NET_2_NET ACCEPT BIDIRECTIONAL</code>	Kommunikation zwischen den an der ersten und zweiten Schnittstelle hängenden Subnetzen ist gestattet

#### Einschränkung der Schnittstelle

Eine Regel kann eingeschränkt werden in Bezug auf die Schnittstelle, über die ein Paket herkam bzw. hinausgeht. Das Format sieht wie folgt aus: `if:in:out`

In der `INPUT`-Kette kann man die Schnittstelle für hinausgehende Pakete nicht einschränken (das Paket geht ja nicht mehr hinaus), in der `POSTROUTING`-Kette kann man die Schnittstelle für hereinkommende Pakete nicht einschränken, da die Information darüber nicht mehr vorhanden ist. Lediglich in der `FORWARD`-Kette kann man für beides Bedingungen angeben.

Möglich sind folgende Werte für *in* bzw. *out*:

- `lo` (Loopback-Schnittstelle, lokale Kommunikation auf dem Router)
- `IP_NET_x_DEV`

- `pppoe` (die PPPoE-Schnittstelle; nur bei entsprechend aktiviertem `dsl`- oder `pppoe_server`-Paket)
- `any`

#### Einschränkungen des Protokolls

Eine Regel kann eingeschränkt werden in Bezug auf das Protokoll, zu dem ein Paket gehört. Das Format sieht wie folgt aus: `prot:protocol` bzw. `prot:icmp:icmp-type`. `protocol` kann dabei einen der folgenden Werte annehmen:

- `tcp`
- `udp`
- `gre` (Generic Routing Encapsulation)
- `icmp` (hier kann man zusätzlich noch einen Namen für den zu filternden ICMP-Typ angeben (`echo-reply` oder `echo-request`), etwa `prot:icmp:echo-request`)
- numerischer Wert der Protokoll-ID (z. B. 41 für IPv6)
- `any`

Wenn eine solche Einschränkung nicht vorhanden ist, aber dennoch Portnummern in einer Regel verwendet werden, dann wird die Regel *zweimal* angelegt, nämlich einmal für das `tcp`- und einmal für das `udp`-Protokoll.

#### Einschränkung der MAC-Adresse

Mittels `mac:mac-address` kann eine Einschränkung bezüglich der MAC-Adresse vorgenommen werden.

#### Einschränkungen in Bezug auf den Zustand eines Paketes

Der von `fi4l` verwendete Paketfilter sammelt Informationen über den Zustand von Verbindungen. Diese Informationen kann man dann nutzen, um Pakete zu filtern, also z. B. nur Pakete durchzulassen, die zu bereits bestehenden Verbindungen gehören. Die Zustände einer Verbindung können sein:<sup>7</sup>

Zustand	Bedeutung
INVALID	Das Paket gehört zu keiner bekannten Verbindung.
ESTABLISHED	Das Paket gehört zu einer Verbindung, über die bereits in beide Richtungen Pakete geflossen sind.
NEW	Das Paket hat eine neue Verbindung aufgebaut oder gehört zu einer Verbindung, bei der noch nicht Pakete in beide Richtungen geflossen sind.

<sup>7</sup>siehe [http://www.sns.ias.edu/~jns/files/iptables\\_talk/x38.htm](http://www.sns.ias.edu/~jns/files/iptables_talk/x38.htm) für eine genauere Beschreibung der Zustände

Zustand	Bedeutung
RELATED	Das Paket baut eine neue Verbindung auf, hat aber eine Beziehung zu einer bestehenden Verbindung (z.B. baut <code>ftp</code> eine separate Verbindung für den eigentlichen Datentransfer auf).

Tabelle 3.6.: Zustandseinschränkungen in Paketfilterregeln

Die Zustände werden wie folgt angegeben: `state:state(s)`. Will man mehrere Zustände angeben, werden diese mit Komma getrennt. Um z. B. nur Pakete durchzulassen, die direkt oder indirekt zu bestehenden Verbindungen gehören, kann man `state:ESTABLISHED,RELATED` schreiben (dies ist in der `INPUT`- oder `FORWARD`-Kette sinnvoll).

### Einschränkung der Häufigkeit einer Aktion

Unter bestimmten Umständen möchte man die Häufigkeit von Aktionen begrenzen, z. B. nur eine ICMP-Echo-Anforderung pro Sekunde zulassen. Das kann man mit der `limit`-Einschränkung erreichen, die wie folgt aussieht: `limit:Häufigkeit:Burst`. Die Häufigkeit wird dabei als  $n/\text{Zeiteinheit}$  (second, minute, hour, day) angegeben, wobei zusätzlich noch Ereignisse gehäuft auftreten können (Burst). Die Angabe `limit:3/minute:5` heißt z. B., dass höchstens drei Ereignisse pro Minute erlaubt sind, wobei auch mal fünf Ereignisse dicht aufeinander folgend akzeptiert werden.

### 3.13.3. Der Einsatz von Schablonen im Paketfilter

Um den Umgang mit dem Paketfilter weiter zu vereinfachen, gibt es die Möglichkeit, häufig vorkommende Regeln zu sogenannten Schablonen (Templates) zusammenzufassen. Damit ist es möglich, eine ganze Reihe von Paketfilterregeln zusammenzufassen und dieser Sammlung von Regeln einen symbolischen Namen zu geben. Anstatt direkt mit Protokollen und Portnummern zu hantieren, verwenden Sie dann Einträge wie `tmpl:ssh`, wenn Sie das `ssh`-Protokoll in einer Regel verwenden wollen. Wie mit Schablonen zu verfahren ist, wird hier am Beispiel von `ssh` gezeigt.

Wollen Sie Ihren `fi4l`-Router vom Internet aus per `ssh` erreichen, so schreiben Sie in einen Eintrag der Array-Variable `PF_INPUT_%` den entsprechenden Dienstnamen (hier `ssh`) mit vorangestelltem `tmpl:` und der Aktion, die für diesen Dienst gelten soll. Beispiel:

```
PF_INPUT_2='tmpl:ssh ACCEPT'
```

Hierbei steht `tmpl:` dafür, dass eine Regel auf einer Schablone basieren soll. Den Namen des Dienstes geben Sie nach dem `:` an, in unserem Beispiel also `ssh`. Zum Schluss geben Sie an, welche Aktion mit dem Dienst verbunden werden soll. Da Sie den `fi4l`-Router aus dem Internet erreichen wollen, erlauben wir die Verbindung mit `ACCEPT`. Einschränkungen von IP-Adressen oder Netzen sind nicht angegeben, also ist der `ssh`-Dienst von allen Netzen und über alle Schnittstellen erreichbar. Sie könnten bei Bedarf die gewohnten Schreibweisen vom Paketfilter benutzen, um den Zugriff auf den `ssh`-Dienst weiter einzuschränken.

Für welche Dienste Regeln vorbereitet sind (d.h. Schablonen existieren), kann in der Schablonen-Datei in `opt/etc/fwrules.tmpl/templates` nachgelesen werden. Im Folgenden finden Sie die Aufstellung in Tabellenform (siehe Tabelle 3.7).

### 3. Basiskonfiguration

Schablone	Protokoll	Port(s)
ad	tcp	389
ad	udp	389
ad	tcp	636
ad	tcp	3268
ad	tcp	3269
ad	udp	88
ad	tcp	88
ad	udp	53
ad	tcp	53
ad	udp	445
ad	tcp	445
ad	tcp	135
ad	tcp	5722
ad	udp	123
ad	udp	464
ad	tcp	464
ad	udp	138
ad	tcp	9389
ad	udp	67
ad	udp	2535
ad	udp	137
ad	udp	139
checkmk	tcp	6556
checkmk	tcp	161
checkmk	udp	161
checkmk	tcp	162
checkmk	udp	162
dhcp	udp	67-68
dns	tcp/udp	53
elster	tcp	159.154.8.2:21
elster	tcp	159.154.8.35:21
elster	tcp	193.109.238.26:8000
elster	tcp	193.109.238.27:8000
elster	tcp	193.109.238.58:80
elster	tcp	193.109.238.59:80
elster	tcp	62.157.211.58:8000
elster	tcp	62.157.211.59:8000
elster	tcp	62.157.211.60:8000
elster	tcp	80.146.179.2:80
elster	tcp	80.146.179.3:80
ftp	tcp	21
http	tcp	80
https	tcp	443
hylafax	tcp	4559
imap	tcp	143
imaps	tcp	993
imond	tcp	5000
ipmi	tcp	22
ipmi	tcp	2937
ipmi	tcp	443
ipmi	tcp	5120
ipmi	tcp	5123
ipmi	tcp	5900
ipmi	tcp	5901
ipmi	tcp	80
ipmi	tcp	8889



### 3. Basiskonfiguration

Schablone	Protokoll	Port(s)
ipmi	udp	623
irc	tcp	6667
ldap	tcp/udp	389
mail	tcp	110
mail	tcp	143
mail	tcp	25
mail	tcp	465
mail	tcp	587
mail	tcp	993
mail	tcp	995
mysql	tcp	3306
nfs	tcp/udp	111
nfs	tcp/udp	2049
nntp	tcp	119
ntp	udp	123
oracle	tcp	1521
pcanywhere	tcp	5631-5632
ping	icmp:0	
ping	icmp:8	
pop3	tcp	110
pop3s	tcp	995
privoxy	tcp	8118
proxmox	tcp	8006
proxmox	tcp	5900
proxmox	tcp	3128
rdp	tcp	3389
rsync	tcp	873
samba	tcp	139
samba	tcp	445
samba	udp	137-138
sip	tcp/udp	5060-5061
smtp	tcp	25
snmp	tcp/udp	161
socks	tcp	1080
squid	tcp	3128
ssh	tcp	22
ssmtp	tcp	465
submission	tcp	587
svn	tcp	3690
syslog	udp	514
teamspeak	tcp	14534
teamspeak	tcp	51234
teamspeak	udp	8767
telmond	tcp	5001
telnet	tcp	23
teredo	udp	3544
tftp	udp	69
time	tcp/udp	37
traceroute	udp	33404-33464
vdr	tcp	6419
vnc	tcp	5900
whois	tcp	43
xbl	tcp/udp	3074
xbl	udp	88
xmppclient	tcp	5222

### 3. Basiskonfiguration

Schablone	Protokoll	Port(s)
xmppserver	tcp	5269

Tabelle 3.7.: Im Lieferumfang von fli4l enthaltene Schablonen

Die Syntax für diese Form der Paketfilterregeln lautet also immer

```
tmpl:<Name des Dienstes> <Einschränkungen> <Gewünschte Aktion>
```

wobei als <Einschränkungen> alles erlaubt ist, was unter [3.13.2](#) beschrieben wird. Die möglichen Werte für <Gewünschte Aktion> sind in [3.13.1](#) aufgelistet und beschrieben.

Ein paar weitere Beispiele sollen die Arbeitsweise verdeutlichen. Zuerst wollen wir uns PF\_PREROUTING ansehen:

```
PF_PREROUTING_N='2'  
PF_PREROUTING_1='tmpl:xbl dynamic DNAT:@xbox'  
PF_PREROUTING_2='tmpl:https dynamic DNAT:192.168.193.250'
```

Die Regel PF\_PREROUTING\_1 versorgt die Xbox mit allem, was für Xbox Live notwendig ist. Im einzelnen werden mit `tmpl:xbl` alle Ports und Protokolle, die für Xbox Live notwendig sind, an den Host `xbox` weitergeleitet. Anstelle der IP-Adresse wird ein Eintrag aus dem `HOST_%_NAME`-Array benutzt. Durch `dynamic` weiß der fli4l, dass die Ports von der Internet-Schnittstelle weitergeleitet werden sollen.

Die zweite Regel leitet das `https`-Protokoll an einen Webserver in der DMZ weiter.

Jetzt sehen wir uns an, wie es mit PF\_INPUT weitergeht:

```
PF_INPUT_N='3'  
PF_INPUT_1='if:IP_NET_1_DEV:any ACCEPT'  
PF_INPUT_2='if:ppoe:any prot:tcp 113 ACCEPT'  
PF_INPUT_3='if:br0:any tmpl:dns @xbox IP_NET_1_IPADDR ACCEPT'
```

Die erste Regel lässt alle aus dem Netz, das mit `IP_NET_1` definiert ist, auf den Router zugreifen. Die zweite Regel ist für das `oident`-Paket. Dort wird der `ident`-Port geöffnet. Die dritte und letzte Regel erlaubt der Xbox den Zugriff auf den DNS Server auf dem fli4l. Hier ist auch wieder schön zu sehen, wie man einen Host-Alias einsetzt.

In PF\_FORWARD und PF\_POSTROUTING steht nichts `tmpl`-spezifisches mehr.

Es ist auch möglich, dass Sie eigene Schablonen anlegen oder dass Pakete ihre eigenen Schablonen mitbringen. Um eine eigene Schablone anzulegen, muss lediglich eine Datei mit den Namen der Schablone erstellt und die entsprechenden Regeln dort aufgenommen werden. Wenn Sie eine private Schablonendatei anlegen wollen, erstellen Sie diese in dem Verzeichnis `etc/fwrules.tmpl` unterhalb Ihres `config`-Verzeichnisses, so wie es die Abbildung [3.2](#) zeigt. Wenn das Verzeichnis `etc/fwrules.tmpl` unterhalb Ihres `config`-Verzeichnisses noch nicht existiert, legen Sie bitte zuerst beide Verzeichnisse an. Alternativ können Paket-Entwickler oder Benutzer, die Schablonen für mehr als eine Konfiguration anlegen wollen, ihre Regeln direkt in das Verzeichnis `opt/etc/fwrules.tmpl` ablegen. In dieses Verzeichnis kommen dann die neuen Schablonen. Dabei gilt die Regel, dass die Schablonen im `config`-Verzeichnis des

### 3. Basiskonfiguration



Abbildung 3.2.: Verzeichnisstruktur fli4l

Benutzers vorrangig behandelt werden. Zum Schluss wird die Schablonendatei, die zum Lieferumfang von fli4l gehört, ausgewertet. Sie können also Einträge in der fli4l-Schablonendatei dadurch „überschreiben“, indem Sie eine Schablonendatei mit dem Namen der zu überschreibenden Schablone in Ihrem `config`-Verzeichnis anlegen.

Wenn Sie zum Beispiel die Schablone `vpn_freunde` anlegen wollen, legen Sie die Datei `vpn_freunde` an. Das Template soll die Dienste `ssh`, `smtp`, `dns` und `samba` enthalten. Also schreiben Sie in die Datei `vpn_freunde` Folgendes:

```
prot:tcp 22
prot:tcp 25
53
prot:udp 137-138
prot:tcp 139
prot:tcp 445
```

Wann immer Sie jetzt die Schablone `vpn_freunde` benutzen, werden daraus Regeln für alle darin aufgeführten Protokolle und Ports erzeugt. `PF_FORWARD_x='tmpl:vpn_freunde ACCEPT'` etwa erstellt folgende FORWARD-Regeln:

```
prot:tcp 22 ACCEPT
prot:tcp 25 ACCEPT
53 ACCEPT
prot:udp 137-138 ACCEPT
prot:tcp 139 ACCEPT
prot:tcp 445 ACCEPT
```

#### 3.13.4. Die Konfiguration des Paketfilters

Der Paketfilter wird im Wesentlichen durch vier Array-Variablen konfiguriert:

- `PF_INPUT_%` konfiguriert die `INPUT`-Kette,
- `PF_FORWARD_%` konfiguriert die `FORWARD`-Kette,
- `PF_OUTPUT_%` konfiguriert die `OUTPUT`-Kette,
- `PF_PREROUTING_%` konfiguriert die `PREROUTING`-Kette und
- `PF_POSTROUTING_%` konfiguriert die `POSTROUTING`-Kette.

Für alle folgenden Ketten gilt die in `PF_LOG_LEVEL` vorgenommene Einstellung der Protokoll-Stufe, deren Inhalt auf einen der folgenden Werte gesetzt werden kann: `debug`, `info`, `notice`, `warning`, `err`, `crit`, `alert`, `emerg`.

##### Die INPUT-Kette

Über die `INPUT`-Kette wird konfiguriert, wer auf den Router zugreifen darf. Trifft keine der Regeln der `INPUT`-Kette zu, bestimmt die Standard-Aktion, was mit dem Paket passieren soll, und die Protokoll-Variable bestimmt, ob es bei einer Ablehnung ins System-Protokoll geschrieben werden soll.

Bei den verwendeten Parametern gibt es die folgenden Einschränkungen:

- Es können nur `ACCEPT`, `DROP` und `REJECT` als Aktion angegeben werden.
- Bei einer Schnittstellen-Einschränkung kann man nur die Eingangsschnittstelle einschränken.

**PF\_INPUT\_POLICY** Diese Variable beschreibt die Standard-Aktion, die angewandt wird, wenn keine der anderen Regeln zutrifft. Möglich sind:

- `ACCEPT` (nicht empfohlen)
- `REJECT`
- `DROP` (nicht empfohlen)

**PF\_INPUT\_ACCEPT\_DEF** Steht diese Variable auf 'yes', werden Standard-Regeln generiert, die für ein korrektes Funktionieren des Routers notwendig sind. Standardmäßig sollte man hier 'yes' eintragen.

Möchte man das Verhalten komplett selbst definieren, kann man hier 'no' eintragen, muss dann jedoch alle Regeln selbst definieren. Eine zum Standardverhalten äquivalente Konfiguration würde wie folgt aussehen (die Beschreibung der Liste für benutzerdefinierte Ketten erfolgt [hier](#) (Seite 64)):

```
PF_INPUT_ACCEPT_DEF='no'
#
# limit ICMP echo requests - use a separate chain
#
```

### 3. Basiskonfiguration

```
PF_USR_CHAIN_N='1'
PF_USR_CHAIN_1_NAME='usr-in-icmp'
PF_USR_CHAIN_1_RULE_N='2'
PF_USR_CHAIN_1_RULE_1='prot:icmp:echo-request length:0-150 limit:1/second:5 ACCEPT'
PF_USR_CHAIN_1_RULE_2='state:RELATED ACCEPT'

PF_INPUT_N='4'
PF_INPUT_1='prot:icmp usr-in-icmp'
PF_INPUT_2='state:ESTABLISHED,RELATED ACCEPT'
PF_INPUT_3='if:lo:any ACCEPT'
PF_INPUT_4='state:NEW 127.0.0.1 DROP BIDIRECTIONAL'
```

Die erste Regel verzweigt zur ratenlimitierenden “usr-in-icmp”-Kette. Die zweite Regel akzeptiert nur solche Pakete, die zu bestehenden Verbindungen gehören (also Paketen, die entweder den Zustand `ESTABLISHED` oder `RELATED` besitzen), und die dritte erlaubt lokale Kommunikation (`if:lo:any ACCEPT`). Die vierte filtert Pakete heraus, die behaupten, lokale Kommunikation zu sein, aber nicht bereits von der vorherigen Regel akzeptiert wurden.

Arbeitet man mit OpenVPN, muss man die Regeln noch ergänzen, um die von diesen Paketen verwendeten Ketten einzubinden.

```
PF_INPUT_N='5'
...
PF_INPUT_5='ovpn-chain'
```

**PF\_INPUT\_LOG** Definiert, ob abgelehnte Pakete vom Kernel protokolliert werden sollen. Dabei können die Meldungen durch Aktivierung von `OPT_KLOGD` über den syslog-Dämon entsprechend der Konfiguration ausgegeben werden.

**PF\_INPUT\_LOG\_LIMIT** Definiert, wie häufig Log-Einträge generiert werden. Die Häufigkeit wird analog zur Limit-Einschränkung als  $n/\text{Zeiteinheit}$  mit Bursts beschrieben, also z. B. `3/minute:5`. Ist dieser Eintrag leer, wird der Standardwert `1/second:5` verwendet; enthält er `none`, wird keine Limitierung durchgeführt.

**PF\_INPUT\_REJ\_LIMIT** **PF\_INPUT\_UDP\_REJ\_LIMIT** Definiert, wie häufig bei einer Ablehnung eines hereinkommenden Paketes auch ein entsprechendes REJECT-Paket generiert wird. Die Häufigkeit wird analog zur Limit-Einschränkung als  $n/\text{Zeiteinheit}$  mit Bursts beschrieben, also z. B. `3/minute:5`. Ist das Limit überschritten, wird das Paket einfach ignoriert (DROP). Ist dieser Eintrag leer, wird der Standardwert `1/second:5` verwendet; enthält er `none`, wird keine Limitierung durchgeführt.

**PF\_INPUT\_ICMP\_ECHO\_REQ\_LIMIT** Definiert, wie häufig auf eine ICMP-Echo-Anfrage reagiert werden soll. Die Häufigkeit wird analog zur Limit-Einschränkung als  $n/\text{Zeiteinheit}$  mit Bursts beschrieben, also z. B. `/minute:5`. Ist das Limit überschritten, wird das Paket einfach ignoriert (DROP). Ist dieser Eintrag leer, wird der Standardwert `1/second:5` verwendet; enthält er `none`, wird keine Limitierung durchgeführt.

**PF\_INPUT\_ICMP\_ECHO\_REQ\_SIZE** Definiert, wie groß eine empfangene ICMP-Echo-Anfrage sein darf (in Bytes). In dieser Angabe sind neben den “Nutzdaten” auch die Paket-Header mit zu berücksichtigen. Der Standard-Wert liegt bei 150 Bytes.

**PF\_INPUT\_N PF\_INPUT\_x PF\_INPUT\_x\_COMMENT** Liste der Regeln, die beschreiben, welche Pakete vom Router angenommen bzw. verworfen werden.

#### Die FORWARD-Kette

Über die FORWARD-Kette wird konfiguriert, welche Pakete vom Router weitergeleitet werden. Trifft keine der Regeln der FORWARD-Kette zu, bestimmt die Standard-Aktion, was mit dem Paket passieren soll, und die Protokoll-Variable bestimmt, ob es bei einer Ablehnung ins System-Protokoll geschrieben werden soll.

Bei den verwendeten Parametern gibt es die Einschränkung, dass nur ACCEPT, DROP und REJECT als Aktion angegeben werden können.

**PF\_FORWARD\_POLICY** Diese Variable beschreibt die Standard-Aktion, die angewandt wird, wenn keine der anderen Regeln zutrifft. Möglich sind:

- ACCEPT
- REJECT
- DROP

**PF\_FORWARD\_ACCEPT\_DEF** Bestimmt, ob der Router Pakete akzeptiert, die zu bestehenden Verbindungen gehören. Steht diese Variable auf 'yes', generiert fli4l automatisch eine Regel, die Pakete mit dem entsprechenden Zustand akzeptiert:

```
'state:ESTABLISHED,RELATED ACCEPT',
```

weiterhin eine Regel, die Pakete mit unbekanntem Zustand verwirft:

```
'state:INVALID DROP'.
```

und schließlich eine Regel, die Pakete mit gefälschten IP-Adressen verwirft:

```
'state:NEW 127.0.0.1 DROP BIDIRECTIONAL'.
```

Zusätzlich generieren die anderen Subsysteme auch noch Standardregeln – eine Konfiguration ohne Standardregeln mit Portweiterleitung und OpenVPN würde mindestens folgende Regeln enthalten:

```
PF_FORWARD_ACCEPT_DEF='no'
PF_FORWARD_N='5'
PF_FORWARD_1='state:ESTABLISHED,RELATED ACCEPT'
PF_FORWARD_2='state:INVALID DROP'
PF_FORWARD_3='state:NEW 127.0.0.1 DROP BIDIRECTIONAL'
PF_FORWARD_4='pfwaccess-chain'
PF_FORWARD_5='ovpn-chain'
```

**PF\_FORWARD\_LOG** Definiert, ob abgelehnte Pakete vom Kernel protokolliert werden sollen. Dabei können die Meldungen durch Aktivierung von OPT\_KLOGD über den syslog-Dämon entsprechend der Konfiguration ausgegeben werden.

**PF\_FORWARD\_LOG\_LIMIT** Definiert, wie häufig Log-Einträge generiert werden. Die Häufigkeit wird analog zur Limit-Einschränkung als  $n/\text{Zeiteinheit}$  mit Bursts beschrieben, also z. B. 3/minute:5. Ist dieser Eintrag leer, wird der Standardwert 1/second:5 verwendet; enthält er none, wird keine Limitierung durchgeführt.

**PF\_FORWARD\_REJ\_LIMIT PF\_FORWARD\_UDP\_REJ\_LIMIT** Definiert, wie häufig bei einer Ablehnung eines hereinkommenden Paketes auch ein entsprechendes REJECT-Paket generiert wird. Die Häufigkeit wird analog zur Limit-Einschränkung als  $n/\text{Zeiteinheit}$  mit Bursts beschrieben, also z. B. `3/minute:5`. Ist das Limit überschritten, wird das Paket einfach ignoriert (DROP). Ist dieser Eintrag leer, wird der Standardwert `1/second:5` verwendet; enthält er `none`, wird keine Limitierung durchgeführt.

**PF\_FORWARD\_N PF\_FORWARD\_x PF\_FORWARD\_x\_COMMENT** Liste der Regeln, die beschreiben, welche Pakete vom Router weitergeleitet bzw. verworfen werden.

#### Die OUTPUT-Kette

Über die OUTPUT-Kette wird konfiguriert, worauf der Router selbst zugreifen darf. Trifft keine der Regeln der OUTPUT-Kette zu, bestimmt die Standard-Aktion, was mit dem Paket passieren soll, und die Protokoll-Variable bestimmt, ob es bei einer Ablehnung ins System-Protokoll geschrieben werden soll.

Bei den verwendeten Parametern gibt es die folgenden Einschränkungen:

- Es können nur ACCEPT, DROP und REJECT als Aktion angegeben werden.
- Bei einer Schnittstellen-Einschränkung kann man nur die Ausgangsschnittstelle einschränken.

**PF\_OUTPUT\_POLICY** Diese Variable beschreibt die Standard-Aktion, die angewandt wird, wenn keine der anderen Regeln zutrifft. Möglich sind:

- ACCEPT
- REJECT
- DROP

**PF\_OUTPUT\_ACCEPT\_DEF** Steht diese Variable auf 'yes', werden Standard-Regeln generiert, die für ein korrektes Funktionieren des Routers notwendig sind. Standardmäßig sollte man hier 'yes' eintragen.

Möchte man das Verhalten komplett selbst definieren, kann man hier 'no' eintragen, muss dann jedoch alle Regeln selbst definieren. Eine zum Standardverhalten äquivalente Konfiguration würde wie folgt aussehen:

```
PF_OUTPUT_ACCEPT_DEF='no'

PF_OUTPUT_N='1'
PF_OUTPUT_1='state:ESTABLISHED,RELATED ACCEPT'
```

Die erste (und einzige) Regel akzeptiert nur solche Pakete, die zu bestehenden Verbindungen gehören (also Paketen, die entweder den Zustand ESTABLISHED oder RELATED besitzen).

**PF\_OUTPUT\_LOG** Definiert, ob abgelehnte Pakete vom Kernel protokolliert werden sollen. Dabei können die Meldungen durch Aktivierung von OPT\_KLOGD über den syslog-Dämon entsprechend der Konfiguration ausgegeben werden.

**PF\_OUTPUT\_LOG\_LIMIT** Definiert, wie häufig Log-Einträge generiert werden. Die Häufigkeit wird analog zur Limit-Einschränkung als  $n/\text{Zeiteinheit}$  mit Bursts beschrieben, also z.B. `3/minute:5`. Ist dieser Eintrag leer, wird der Standardwert `1/second:5` verwendet; enthält er `none`, wird keine Limitierung durchgeführt.

**PF\_OUTPUT\_REJ\_LIMIT PF\_OUTPUT\_UDP\_REJ\_LIMIT** Definiert, wie häufig bei einer Ablehnung eines hereinkommenden Paketes auch ein entsprechendes REJECT-Paket generiert wird. Die Häufigkeit wird analog zur Limit-Einschränkung als  $n/\text{Zeiteinheit}$  mit Bursts beschrieben, also z.B. `3/minute:5`. Ist das Limit überschritten, wird das Paket einfach ignoriert (DROP). Ist dieser Eintrag leer, wird der Standardwert `1/second:5` verwendet; enthält er `none`, wird keine Limitierung durchgeführt.

**PF\_OUTPUT\_N PF\_OUTPUT\_x PF\_OUTPUT\_x\_COMMENT** Liste der Regeln, die beschreiben, welche Pakete vom Router versandt bzw. verworfen werden.

#### Benutzerdefinierte Listen

Aus verschiedenen Gründen besteht manchmal der Bedarf, eigene Ketten anzulegen und dort die Pakete genauer zu filtern. Diese Ketten kann man mittels `PF_USR_CHAIN_%` definieren und mit Regeln füllen. Die Namen der Ketten müssen dabei mit *usr-* beginnen und können nach ihrer Definition überall in der INPUT- oder FORWARD-Kette statt einer Aktion eingesetzt werden. Als Beispiel soll hier die bereits vorher verwendete ICMP-Filterkette dienen:

```
PF_USR_CHAIN_N='1'
#
# create usr-in-icmp
#
PF_USR_CHAIN_1_NAME='usr-in-icmp'
#
# add rule to usr-in-icmp
#
PF_USR_CHAIN_1_RULE_N='2'
PF_USR_CHAIN_1_RULE_1='prot:icmp:echo-request length:0-150 limit:1/second:5 ACCEPT'
PF_USR_CHAIN_1_RULE_2='state:RELATED ACCEPT'
#
# use chain in PF_INPUT
#
PF_INPUT_2='prot:icmp usr-in-icmp'
```

**PF\_USR\_CHAIN\_N** Definiert die Anzahl der benutzerdefinierten Ketten.

**PF\_USR\_CHAIN\_x\_NAME** Definiert den Namen der benutzerdefinierten Kette. Dieser muss mit *usr-* beginnen.

**PF\_USR\_CHAIN\_x\_RULE\_N**

**PF\_USR\_CHAIN\_x\_RULE\_x**

**PF\_USR\_CHAIN\_x\_RULE\_x\_COMMENT** Hier werden die Regeln definiert, die in die benutzerdefinierte Kette eingefügt werden sollen. Es können alle Regeln verwendet werden, die auch in einer FORWARD-Kette verwendet werden könnten. Sollte keine Regel der benutzerdefinierten Kette zutreffen, wird zur Ausgangskette zurückgekehrt und mit der Regel nach der Verzweigung fortgefahren.



#### Die NAT-Ketten (Network Address Translation)

Pakete können vor und nach Routing-Entscheidungen noch manipuliert werden. Sie können zum Beispiel eine neue Zieladresse erhalten, um an einen anderen Rechner weitergeleitet zu werden (Portweiterleitung) oder eine andere Quelladresse erhalten, um das hinter dem Router liegende Netzwerk zu maskieren. Maskieren nutzt man beispielsweise, um ein privates Netz über eine öffentliche IP ins Netz zu bringen oder in einem DMZ-Setup die Struktur des lokalen Netzes vor den Rechnern in der DMZ zu verbergen.

Die Konfiguration erfolgt über zwei Ketten, die `PREROUTING`- und die `POSTROUTING`-Kette. Über die `POSTROUTING`-Kette wird konfiguriert, welche Pakete vom Router maskiert werden. Trifft keine der Regeln der `POSTROUTING`-Kette zu, werden die Pakete unmaskiert weitergeleitet.

Beim Maskieren gibt es zwei Varianten: eine für Netzwerk-Schnittstellen, die bei der Auswahl erst eine IP-Adresse zugewiesen bekommen (`MASQUERADE`) und eine für Netzwerk-Schnittstellen mit statischer IP-Adresse (`SNAT`). `SNAT` erwartet dabei zusätzlich die IP-Adresse, die im Paket als Quelle eingetragen werden soll. Diese kann als

- IP-Adresse (Beispiel: `SNAT:1.2.3.4`),
- IP-Bereich (Beispiel: `SNAT:1.2.3.4-1.2.3.10`)
- oder als symbolische Referenz (Beispiel: `SNAT:IP_NET_1_IPADDR`)

angegeben werden.

Sowohl bei `SNAT` als auch bei `MASQUERADE` kann schließlich ein Port bzw. Portbereich angegeben werden, auf den der Quellport abgebildet werden soll. Normalerweise ist das nicht nötig, da der Kern die Ports allein auswählen kann. Es gibt aber Anwendungen, die verlangen, dass der Quellport unverändert bleibt (und somit ein 1:1-NAT erfordern) oder die ein PAT (Port Address Translation) oder NAT (Network Address and Port Translation) verbieten. Der Portbereich wird einfach hinten angehängt, z. B. so: `SNAT:IP_NET_1_IPADDR:4000-8000`.

Bei der `POSTROUTING`-Kette können nur `ACCEPT`, `SNAT`, `NETMAP` und `MASQUERADE` als Aktionen verwendet werden.

#### `PF_POSTROUTING_N PF_POSTROUTING_x PF_POSTROUTING_x_COMMENT`

Eine Liste der Regeln, die beschreiben, welche Pakete vom Router maskiert werden (bzw. unmaskiert weitergeleitet werden). Will man Pakete vom Maskieren ausklammern, kann man eine `ACCEPT`-Regel für die auszuklammernden Pakete der `MASQUERADE`-Regel voranstellen.

Über die `PREROUTING`-Kette wird konfiguriert, welche Pakete an einen anderen Rechner weitergeleitet werden sollen. Trifft keine der Regeln der `PREROUTING`-Kette zu, werden die Pakete unverändert weiterbehandelt. Die Aktion `DNAT` erwartet dabei die IP-Adresse, die im Paket als Ziel eingetragen werden soll. Diese kann als

- IP-Adresse (Beispiel: `DNAT:1.2.3.4`),
- IP-Bereich (Beispiel: `DNAT:1.2.3.4-1.2.3.10`)
- oder als Hostname (Beispiel: `DNAT:@client1`)

angegeben werden.

Schließlich kann noch ein Port bzw. Portbereich angegeben werden, auf den der Zielport abgebildet werden soll. Das ist aber nur nötig, wenn der Port geändert werden soll. Der Port bzw. Portbereich wird einfach hinten angehängt, z. B. so: DNAT:@server:21.

REDIRECT verhält sich wie DNAT, nur dass die Ziel-IP-Adresse immer auf die (primäre) IP-Adresse der Schnittstelle, auf der das Paket hereinkam, gesetzt wird und damit das Paket lokal zugestellt wird. Dies wird z. B. für transparente Proxys benötigt, siehe OPT\_TRANSPROXY (Seite ??).

Will man eine Portweiterleitung auf Schnittstellen mit dynamischen Adressen machen, weiß man zum Zeitpunkt der Konfiguration noch nicht, an welche IP die Pakete gerichtet sein werden. Daher kann man in der PREROUTING-Kette **dynamic** als Platzhalter für die später zugewiesene IP verwenden, etwa wie folgt:

```
'dynamic:80 DNAT:1.2.3.4'          # leite http-Pakete an die
                                   # IP-Adresse 1.2.3.4 weiter
'prot:gre any dynamic DNAT:1.2.3.4' # leite gre-Pakete (Teil des PPTP-
                                   # Protokolls) an die IP-Adresse
                                   # 1.2.3.4 weiter
```

Bei der PREROUTING-Kette können nur ACCEPT, DNAT, NETMAP und REDIRECT als Aktionen verwendet werden.

Für weitere Beispiele zur Portweiterleitung siehe den nächsten Abschnitt.

#### **PF\_PREROUTING\_N PF\_PREROUTING\_x PF\_PREROUTING\_x\_COMMENT**

Eine Liste der Regeln, die beschreiben, welche Pakete vom Router an ein anderes Ziel weitergeleitet werden sollen.

#### **3.13.5. Beispiele**

Im Folgenden sind einige Beispiele für die Paketfilter-Konfiguration angegeben.

##### **Die fli4l-Standardkonfiguration**

Die fli4l-Standardkonfiguration der Distribution sieht für die INPUT-Kette wie folgt aus:

```
PF_INPUT_POLICY='REJECT'
PF_INPUT_ACCEPT_DEF='yes'
PF_INPUT_LOG='no'
PF_INPUT_N='1'
PF_INPUT_1='IP_NET_1 ACCEPT'
```

Damit erreichen wir, dass

- Rechner im lokalen Netzwerk auf den Router zugreifen dürfen (PF\_INPUT\_1='IP\_NET\_1 ACCEPT'),
- lokale Kommunikation auf dem Router erlaubt ist (PF\_INPUT\_ACCEPT\_DEF='yes'),
- Pakete, die zu vom Router aufgebauten Verbindungen gehören, akzeptiert werden (PF\_INPUT\_ACCEPT\_DEF='yes'),

### 3. Basiskonfiguration

- alles andere abgelehnt wird (PF\_INPUT\_POLICY='REJECT'),
- aber nicht ins System-Protokoll geschrieben wird (PF\_INPUT\_LOG='no').

Für die FORWARD-Kette sieht das so ähnlich aus: Nur Pakete unseres lokalen Netzes und Pakete, die zu Verbindungen gehören, die von Rechnern im lokalen Netz aufgebaut wurden, sollen weitergeleitet werden. Des Weiteren werden NetBIOS- und CIFS-Pakete verworfen.

```
PF_FORWARD_POLICY='REJECT'
PF_FORWARD_ACCEPT_DEF='yes'
PF_FORWARD_LOG='no'
PF_FORWARD_N='2'
PF_FORWARD_1='tmp1:samba DROP'
PF_FORWARD_2='IP_NET_1 ACCEPT'
```

Was man hier gut sieht, ist die Abhängigkeit von der Reihenfolge der Regeln: *Zuerst* werden NetBIOS-Pakete verworfen, und *danach* werden die Pakete des lokalen Netzes akzeptiert.

Nun kann das lokale Netz mit dem Router kommunizieren, seine Pakete werden weitergeleitet, es fehlt nur noch das Maskieren, welches für den Zugriff eines privaten Netzwerkes auf das Internet notwendig ist:

```
PF_POSTROUTING_N='1'
PF_POSTROUTING_1='IP_NET_1 MASQUERADE'
```

#### Trusted Nets

Wollen wir lokal mehrere Subnetze haben, die frei und unmaskiert miteinander kommunizieren können, müssen wir dafür sorgen, dass Pakete zwischen diesen Subnetzen nicht verworfen und auch nicht maskiert werden. Dazu fügen wir einfach eine Regel hinzu oder modifizieren die vorhandene.

Angenommen, wir haben einen DSL-Zugang über PPPoE, und die beiden Subnetze sind IP\_NET\_1 (192.168.6.0/24) und IP\_NET\_2 (192.168.7.0/24). Dann würde die Konfiguration wie folgt aussehen:

```
PF_FORWARD_POLICY='REJECT'
PF_FORWARD_ACCEPT_DEF='yes'
PF_FORWARD_LOG='no'
PF_FORWARD_N='4'
PF_FORWARD_1='IP_NET_1 IP_NET_2 ACCEPT BIDIRECTIONAL'
PF_FORWARD_2='tmp1:samba DROP'
PF_FORWARD_3='IP_NET_1 ACCEPT'
PF_FORWARD_4='IP_NET_2 ACCEPT'

PF_POSTROUTING_N='3'
PF_POSTROUTING_1='IP_NET_1 IP_NET_2 ACCEPT BIDIRECTIONAL'
PF_POSTROUTING_2='IP_NET_1 MASQUERADE'
PF_POSTROUTING_3='IP_NET_2 MASQUERADE'
```

Regel eins sorgt jetzt dafür, dass Pakete zwischen den beiden Subnetzen ohne weitere Prüfung weitergeleitet werden. Die Regeln drei und vier sorgen dafür, dass beide Subnetze auch ins Internet kommen. Die erste Regel der POSTROUTING-Kette sorgt dafür, dass die Kommunikation zwischen den Subnetzen unmaskiert erfolgt.

### 3. Basiskonfiguration

Alternativ könnten wir auch sagen, dass nur Pakete, die über die **pppoe**-Schnittstelle hinausgehen, maskiert werden sollen:

```
PF_POSTROUTING_N='1'  
PF_POSTROUTING_1='if:any:pppoe MASQUERADE'
```

Genauso hätte man die Filterung der Ports auch auf die **pppoe**-Schnittstelle beschränken und die beiden Subnetze zu einem zusammenfassen können, das würde dann wie folgt aussehen:

```
PF_FORWARD_POLICY='REJECT'  
PF_FORWARD_ACCEPT_DEF='yes'  
PF_FORWARD_LOG='no'  
PF_FORWARD_N='2'  
PF_FORWARD_1='if:any:pppoe tmpl:samba DROP'  
PF_FORWARD_2='192.168.6.0/23 ACCEPT'
```

```
PF_POSTROUTING_N='1'  
PF_POSTROUTING_1='if:any:pppoe MASQUERADE'
```

Pakete, die über die **pppoe**-Schnittstelle hinausgehen und die an die **udp**-Ports 137-138 oder an die **tcp**-Ports 139 und 445 adressiert sind, werden verworfen (Regel 1), alle anderen Pakete, die aus dem Subnetz 192.168.6.0/23 kommen, werden weitergeleitet (Regel 2).

#### Route Network

Fügen wir dem Ganzen noch ein Netzwerk 10.0.0.0/24 hinzu (z. B. ein Dial-In-Netzwerk), mit dem wir unmaskiert kommunizieren wollen, wobei Pakete an die **udp**-Ports 137-138 sowie an die **tcp**-Ports 139 und 445 verworfen werden sollen, dann würde das wie folgt aussehen:

```
PF_FORWARD_POLICY='REJECT'  
PF_FORWARD_ACCEPT_DEF='yes'  
PF_FORWARD_LOG='no'  
PF_FORWARD_N='4'  
PF_FORWARD_1='IP_NET_1 IP_NET_2 ACCEPT BIDIRECTIONAL'  
PF_FORWARD_2='tmpl:samba DROP'  
PF_FORWARD_3='192.168.6.0/23 ACCEPT'  
PF_FORWARD_4='10.0.0.0/24 ACCEPT'  
  
PF_POSTROUTING_N='2'  
PF_POSTROUTING_1='10.0.0.0/24 ACCEPT BIDIRECTIONAL'  
PF_POSTROUTING_2='192.168.6.0/23 MASQUERADE'
```

- Regel 1 erlaubt die ungehinderte Kommunikation zwischen den Subnetzen **IP\_NET\_1** und **IP\_NET\_2**.
- Regel 2 verwirft Pakete an die Samba-Ports.
- Die Regeln 3 und 4 erlaubt die Weiterleitung von Paketen, die aus den Subnetzen 192.168.6.0/24, 192.168.7.0/24 und 10.0.0.0/24 kommen; die Rückrichtung wird von der Einstellung **PF\_FORWARD\_ACCEPT\_DEF='yes'** abgedeckt.
- Regel 1 der **POSTROUTING**-Kette sorgt dafür, dass Pakete in das bzw. aus dem 10.0.0.0/24-Subnetz nicht maskiert werden.

### 3. Basiskonfiguration

Alternativ ginge auch:

```
PF_POSTROUTING_N='1'  
PF_POSTROUTING_1='if:any:pppoe MASQUERADE'
```

Diese Regel besagt, dass nur Pakete, die über die **pppoe**-Schnittstelle hinausgehen, maskiert werden.

#### Blacklists, Whitelists

Blacklists (ein Rechner in dieser Liste darf etwas nicht) und Whitelists (ein Rechner in dieser Liste darf etwas) werden prinzipiell ähnlich umgesetzt. Es werden Regeln geschrieben, die am Anfang sehr speziell sind und nach hinten immer allgemeiner werden. Bei einer Blacklist stehen am Anfang Regeln, die etwas verbieten und am Ende Regeln, die allen bisher nicht erwähnten etwas erlauben. Bei einer Whitelist ist es genau umgekehrt.

*Beispiel 1:* Alle Rechner im Subnetz 192.168.6.0/24 außer Rechner 12 dürfen ins Internet, solange sie nicht mit den CIFS Ports 137-138 (**udp**), 139 und 445 (**tcp**) kommunizieren wollen:

```
PF_FORWARD_POLICY='REJECT'  
PF_FORWARD_ACCEPT_DEF='yes'  
PF_FORWARD_LOG='no'  
PF_FORWARD_N='3'  
PF_FORWARD_1='192.168.6.12 DROP'  
PF_FORWARD_2='tmpl:samba DROP'  
PF_FORWARD_3='192.168.6.0/23 ACCEPT'  
  
PF_POSTROUTING_N='1'  
PF_POSTROUTING_2='192.168.6.0/24 MASQUERADE'
```

*Beispiel 2:* Nur Rechner 12 darf ins Internet (aber nicht an die o.g. Ports ...), alle anderen dürfen nur lokal mit einem anderen Subnetz kommunizieren:

```
PF_FORWARD_POLICY='REJECT'  
PF_FORWARD_ACCEPT_DEF='yes'  
PF_FORWARD_LOG='no'  
PF_FORWARD_N='3'  
PF_FORWARD_1='192.168.6.0/24 192.168.7.0/24 ACCEPT BIDIRECTIONAL'  
PF_FORWARD_2='tmpl:samba DROP'  
PF_FORWARD_3='192.168.6.12 ACCEPT'  
  
PF_POSTROUTING_N='1'  
PF_POSTROUTING_1='if:any:pppoe MASQUERADE'
```

#### 3.13.6. Standardkonfigurationen

##### Einfacher maskierender Router mit einem Netz dahinter

```
#  
# Zugriff auf den Router  
#  
PF_INPUT_POLICY='REJECT'  
PF_INPUT_ACCEPT_DEF='yes'
```

### 3. Basiskonfiguration

```
PF_INPUT_LOG='no'
PF_INPUT_N='1'
PF_INPUT_1='IP_NET_1 ACCEPT'    # alle Hosts im lokalen Netz dürfen
                                # auf den Router zugreifen

#
# Zugriff auf das ``Internet''
#
PF_FORWARD_POLICY='REJECT'
PF_FORWARD_ACCEPT_DEF='yes'
PF_FORWARD_LOG='no'

PF_FORWARD_N='2'
PF_FORWARD_1='tmpl:samba DROP' # Samba-Pakete, die das Netz
                                # verlassen wollen, werden verworfen
PF_FORWARD_2='IP_NET_1 ACCEPT' # alle anderen Pakete dürfen das
                                # lokale Netz verlassen

#
# Maskieren des lokalen Netzes
#
PF_POSTROUTING_N='1'
PF_POSTROUTING_1='IP_NET_1 MASQUERADE' # maskiere Pakete, die das Subnetz
                                         # verlassen
```

#### Einfacher maskierender Router mit zwei Netzen dahinter

```
#
# Zugriff auf den Router
#
PF_INPUT_POLICY='REJECT'
PF_INPUT_ACCEPT_DEF='yes'
PF_INPUT_LOG='no'
PF_INPUT_N='2'
PF_INPUT_1='IP_NET_1 ACCEPT'    # alle Hosts im lokalen Netz dürfen
                                # auf den Router zugreifen
PF_INPUT_2='IP_NET_2 ACCEPT'    # alle Hosts im lokalen Netz dürfen
                                # auf den Router zugreifen

#
# Zugriff auf das ``Internet''
#
PF_FORWARD_POLICY='REJECT'
PF_FORWARD_ACCEPT_DEF='yes'
PF_FORWARD_LOG='no'

#
# Freie Kommunikation zwischen den Netzen
#
PF_FORWARD_N='4'
PF_FORWARD_1='IP_NET_1 IP_NET_2 ACCEPT BIDIRECTIONAL'
PF_FORWARD_2='tmpl:samba DROP' # Samba-Pakete, die das Netz
                                # verlassen wollen, werden verworfen
```

### 3. Basiskonfiguration

```
PF_FORWARD_3='IP_NET_1 ACCEPT' # alle anderen Pakete dürfen das
                                # lokale Netz verlassen
PF_FORWARD_4='IP_NET_2 ACCEPT' # alle anderen Pakete dürfen das
                                # lokale Netz verlassen

#
# Maskieren der lokalen Netze, unmaskierte Kommunikation zwischen den
# Netzen
#
PF_POSTROUTING_N='3'
PF_POSTROUTING_1='IP_NET_1 IP_NET_2 ACCEPT BIDIRECTIONAL'
PF_POSTROUTING_2='IP_NET_1 MASQUERADE' # maskiere Pakete, die das Subnetz
                                        # verlassen
PF_POSTROUTING_3='IP_NET_2 MASQUERADE' # maskiere Pakete, die das Subnetz
                                        # verlassen
```

#### **Maskierender DSL-Router mit zwei Netzen dahinter und SSH/HTTP-Zugriff aus dem Internet**

```
#
# Zugriff auf den Router
#
PF_INPUT_POLICY='REJECT'
PF_INPUT_ACCEPT_DEF='yes'
PF_INPUT_LOG='no'
PF_INPUT_N='4'
PF_INPUT_1='IP_NET_1 ACCEPT' # alle Hosts im lokalen Netz dürfen
                              # auf den Router zugreifen
PF_INPUT_2='IP_NET_2 ACCEPT' # alle Hosts im lokalen Netz dürfen
                              # auf den Router zugreifen
PF_INPUT_3='tmpl:ssh ACCEPT' # gestatte Zugriff auf SSH-Dienst
                              # von überall her
PF_INPUT_4='tmpl:http 1.2.3.4/24 ACCEPT' # gestatte Rechner aus
                                          # einem bestimmten Subnetz Zugriff
                                          # auf HTTP-Dienst

#
# Zugriff auf das ``Internet''
#
PF_FORWARD_POLICY='REJECT'
PF_FORWARD_ACCEPT_DEF='yes'
PF_FORWARD_LOG='no'

#
# Keine Kommunikation zwischen den Netzen, beide Netze dürfen ins
# Internet, Samba-Pakete werden verworfen
#
PF_FORWARD_N='2'
PF_FORWARD_1='tmpl:samba if:any:pppoe DROP' # Samba-Pakete, die das Netz
                                              # verlassen wollen, werden verworfen
PF_FORWARD_2='if:any:pppoe ACCEPT' # alle anderen Pakete dürfen das
                                    # lokale Netz verlassen
```

### 3. Basiskonfiguration

```
#
# Maskieren der lokalen Netze, unmaskierte Kommunikation zwischen den
# Netzen
#
PF_POSTROUTING_N='1'
PF_POSTROUTING_1='if:any:pppoe MASQUERADE' # maskiere Pakete, die das Subnetz
                                           # verlassen
```

#### Portweiterleitung

Portweiterleitungen lassen sich mit den PREROUTING-Regeln wie folgt umsetzen (TARGET bezeichnet die ursprüngliche Zieladresse (optional) und den ursprünglichen Zielpport, NEW\_TARGET bezeichnet die neue Zieladresse und den neuen Zielpport (optional), PROTOCOL bezeichnet das jeweilige Protokoll):

```
TARGET='<port>'
NEW_TARGET='<ip>'
PROTOCOL='<proto>'
PF_PREROUTING_x='prot:<proto> dynamic:<port> DNAT:<ip>'

TARGET='<port1>-<port2>'
NEW_TARGET='<ip>'
PROTOCOL='<proto>'
PF_PREROUTING_x='prot:<proto> dynamic:<port1>-<port2> DNAT:<ip>'

TARGET='<ip>:<port-a>'
NEW_TARGET='<ip>:<port-b>'
PROTOCOL='<proto>'
PF_PREROUTING_x='prot:<proto> any <ip>:<port-a> DNAT:<ip>:<port-b>'
```

#### Transparenter Proxy

Will man bestimmte Zugriffe auf das Internet nur über einen lokalen Proxy zulassen, kann man das mit Hilfe der PREROUTING- und POSTROUTING-Ketten erzwingen, ohne dass der Client davon etwas merkt. Prinzipiell sind dazu drei Schritte notwendig:

1. Anfragen an den HTTP-Port, die nicht vom Proxy kommen, an den Proxy umleiten (PREROUTING).
2. Die umgeleiteten Pakete so verändern, dass der Proxy denkt, sie kommen vom Router, so dass er sie wieder dorthin zurückschickt (POSTROUTING).
3. Die Pakete durch die FORWARD-Kette durchlassen, sofern ein Eintrag à la

```
PF_FORWARD_x='IP_NET_1 ACCEPT'
```

nicht existiert (FORWARD).

*Beispiel 1:* Angenommen, wir haben nur ein Netz IP\_NET\_1, in dem auf einem Rechner namens proxy ein Squid-Proxy läuft, und wollen den gesamten http-Datenverkehr über ihn



### 3. Basiskonfiguration

leiten. Squid lauscht auf Port 3128. Der Einfachheit halber beziehen wir uns via `@proxy` auf den eingetragenen Host aus `HOST_1_NAME='proxy'` (vgl. [Domainkonfiguration](#) (Seite 82)).

Das Ganze würde wie folgt aussehen:

```
...
PF_PREROUTING_x='@proxy ACCEPT'
    # Pakete vom Proxy sollen nicht umgeleitet werden

PF_PREROUTING_x='prot:tcp IP_NET_1 80 DNAT:@proxy:3128'
    # HTTP-Pakete aus IP_NET_1 mit einem beliebigen Ziel werden
    # umgeleitet nach @proxy, Port 3128

PF_POSTROUTING_x='any @proxy:3128 SNAT:IP_NET_1_IPADDR'
    # alle Pakete an den Proxy-Port 3128 so umschreiben, als wären sie
    # vom fli4l (IP_NET_1_IPADDR)

PF_FORWARD_x='prot:tcp @proxy 80 ACCEPT'
    # HTTP-Pakete vom Proxy durch die FORWARD-Kette durchlassen (wenn nötig)
...
```

Gibt es mehrere Netze oder potentielle Konflikte mit anderen Portweiterleitungen (die ja auch nichts anderes sind als DNAT-Regeln), muss man die Regeln vielleicht noch etwas enger formulieren.

*Beispiel 2:* Unser Proxy namens `proxy` steht in `IP_NET_1`, lauscht auf Port 3128 und soll nur für Clients aus `IP_NET_1` wirksam werden. `IP_NET_1` ist über `IP_NET_1_DEV` erreichbar. Pakete aus weiteren Netzen sollen nicht berücksichtigt werden.

```
...
PF_PREROUTING_x='if:IP_NET_1_DEV:any !@proxy 80 DNAT:@proxy:3128'
    # Anfragen an den HTTP-Port, die nicht vom Proxy, aber über eine
    # interne Schnittstelle (IP_NET_1_DEV) kommen, an den Proxy-Port umleiten.
    # An dieser Stelle ist es wichtig, mit if:IP_NET_1_DEV:any zu
    # überprüfen, ob die Pakete von innen kommen, da sonst auch Pakete von
    # außen umgeleitet würden (Sicherheitslücke!).

PF_POSTROUTING_x='prot:tcp IP_NET_1 @proxy:3128 SNAT:IP_NET_1_IPADDR'
    # HTTP-Pakete die aus IP_NET_1 stammen und für den Proxy-Port 3128
    # gedacht sind, so umschreiben, als wären sie vom fli4l (IP_NET_1_IPADDR)

PF_FORWARD_x='prot:tcp @proxy 80 ACCEPT'
    # HTTP-Pakete vom Proxy durch die FORWARD-Kette durchlassen (wenn nötig)
...
```

*Beispiel 3:* Um sich das Leben etwas zu erleichtern und die Regeln kürzer zu gestalten, kann man auch Templates einsetzen (vgl. [Templates im Paketfilter](#) (Seite 55)). Zweckmäßig ist an dieser Stelle das `tmpl:http`, das in `prot:tcp any any:80` übersetzt wird. So wird z. B. aus `tmpl:http IP_NET_1 DNAT:@proxy:3128` dann `prot:tcp IP_NET_1 80 DNAT:@proxy:3128`.

Sowohl `IP_NET_1` als auch `IP_NET_2` sollen transparent über den Proxy umgeleitet werden. Damit ließe sich vereinfacht auch schreiben:

```
...
```

### 3. Basiskonfiguration

```
PF_PREROUTING_x='tmpl:http @proxy ACCEPT'
    # HTTP-Pakete vom Proxy sollen nicht umgeleitet werden

PF_PREROUTING_x='tmpl:http IP_NET_1 DNAT:@proxy:3128'
    # HTTP-Pakete aus IP_NET_1 sollen umgeleitet werden

PF_PREROUTING_x='tmpl:http IP_NET_2 DNAT:@proxy:3128'
    # HTTP-Pakete aus IP_NET_2 sollen umgeleitet werden

PF_POSTROUTING_x='IP_NET_1 @proxy:3128 SNAT:IP_NET_1_IPADDR'
PF_POSTROUTING_x='IP_NET_2 @proxy:3128 SNAT:IP_NET_2_IPADDR'

PF_FORWARD_x='tmpl:http @proxy ACCEPT'
...
```

Und so ließe sich das endlos fortsetzen ...

#### 3.13.7. DMZ – Demilitarisierte Zone

fi4l gestattet auch den Aufbau einer DMZ. Hier sei erstmal auf das Wiki verwiesen. <https://ssl.networks.org/wiki>

#### 3.13.8. Conntrack-Helfer

Die Verwendung von IP-Masquerading hat zwar den Vorteil, dass mehrere Rechner im LAN über eine einzige offizielle IP-Adresse geroutet werden kann, es gibt aber auch Nachteile, die man in Kauf nehmen muss.

Ein großes Problem ist zum Beispiel, dass kein Rechner von außen von sich aus eine Verbindung zu einem Rechner aufnehmen kann. Das ist zwar aus Sicherheitsgründen eigentlich durchaus erwünscht, aber bestimmte Protokolle funktionieren nicht mehr, weil sie einen Verbindungsaufbau von außen einfach erfordern.

Ein klassisches Beispiel ist FTP. Neben dem Kommunikationskanal, auf dem Befehle und Antworten ausgetauscht werden, wird ein weiterer Kanal (in Form eines IP-Ports) verwendet, um die eigentlichen Nutzdaten zu versenden. fi4l verwendet dafür bestimmte Conntrack-Helfer, um solche zusätzlichen Ports, die verwendet werden, ad hoc dann freizuschalten und an den internen Rechner weiterzuleiten, wenn sie benötigt werden. Dabei “horcht” der Conntrack-Helfer in den Datenstrom, um zu erkennen, wann ein zusätzlicher Port benötigt wird.

Typische Anwendungen für Conntrack-Helfer sind Chat-Protokolle und Spiele im Internet.

Ein solcher Conntrack-Helfer wird über Regeln in zwei speziellen Arrays aktiviert. Das Array `PF_PREROUTING_CT_%` enthält Helfer-Zuordnungen zu Paketen, die von außen kommen, das Array `PF_OUTPUT_CT_%` enthält Helfer-Zuordnungen zu Paketen, die auf dem Router generiert werden. Einige Beispiele aus der Praxis sollen dies verdeutlichen.

*Beispiel 1:* Soll aktives FTP aus dem LAN erlaubt werden, ist das aus der Sicht des Routers eine Verbindung von außerhalb, somit muss ein Eintrag in `PF_PREROUTING_CT_%` vorgenommen werden:

```
PF_PREROUTING_CT_N='1'
PF_PREROUTING_CT_1='tmpl:ftp IP_NET_1 HELPER:ftp'
```

### 3. Basiskonfiguration

Damit wird für alle TCP-Verbindungen aus dem lokalen Netz (`IP_NET_1`) zu irgendeiner anderen Adresse an Port 21 (dies ist der `ftp`-Port) das `ftp`-Hilfsmodul geladen. Dieses Modul erlaubt dann im Laufe der Verbindung, dass der FTP-Server zurück zum Client eine Datenverbindung aufbauen kann, indem temporär ein "Loch" in der Firewall aufgemacht wird.

*Beispiel 2:* Soll passives FTP für einen FTP-Server im LAN ermöglicht werden (dabei wird die Datenverbindung von außen nach innen aufgebaut, so dass auch hier kurzfristig ein Loch in der Firewall geöffnet werden muss), ist dies ebenfalls aus der Sicht des Router eine Verbindung von außerhalb des Routers. Hier sieht die Regel folgendermaßen aus:

```
PF_PREROUTING_CT_N='1'  
PF_PREROUTING_CT_1='tmpl:ftp any dynamic HELPER:ftp'
```

Mit dieser Regel wird ausgedrückt, dass alle FTP-Verbindungen, die an die dynamische Adresse des Routers gesandt werden, mit dem FTP-Conntrack-Helfer assoziiert werden. Hier wurde `dynamic` verwendet, da angenommen wird, dass der Router für die Einwahl ins Internet verantwortlich ist und somit eine externe IP-Adresse besitzt. Falls der Router eine Einwahl via DSL durchführt, kann man die Regel auch so schreiben:

```
PF_PREROUTING_CT_N='1'  
PF_PREROUTING_CT_1='tmpl:ftp if:pppoe:any HELPER:ftp'
```

Mit dieser Regel wird ausgedrückt, dass alle FTP-Verbindungen, die von der DSL-Schnittstelle (`pppoe`) kommen, mit dem FTP-Conntrack-Helfer assoziiert werden.

Falls der Router sich nicht einwählt, sondern z. B. hinter einem anderen Router (Fritz!Box, Kabelmodem etc.) hängt, so kann die folgende Regel verwendet werden:

```
PF_PREROUTING_CT_N='1'  
PF_PREROUTING_CT_1='tmpl:ftp if:IP_NET_2_DEV:any HELPER:ftp'
```

Dabei wird im Beispiel angenommen, dass die Verbindung zum anderen Router über die Schnittstelle durchgeführt wird, die dem zweiten Subnetz zugeordnet ist (`IP_NET_2_DEV`).

Zu beachten ist, dass natürlich *zusätzlich* eine entsprechende Konfiguration der FORWARD-Kette nötig ist, um die FTP-Pakete auch tatsächlich weiterzuleiten. Eine typische Regel wäre etwa

```
PF_PREROUTING_1='tmpl:ftp any dynamic DNAT:@ftpserver'
```

wobei angenommen wird, dass der Host, auf dem das FTP-Serverprogramm läuft, den Namen `ftpserver` hat.

*Beispiel 3:* Schließlich muss auch, wenn man vom fl4l direkt aktives FTP benutzen möchte (etwa mit Hilfe des `ftp`-Programms aus dem `tools`-Paket), die Firewall dafür vorbereitet werden, diesmal in der OUTPUT-Kette, die mit Hilfe des Arrays `PF_OUTPUT_CT_%` konfiguriert wird:

```
PF_OUTPUT_CT_N='1'  
PF_OUTPUT_CT_1='tmpl:ftp HELPER:ftp'
```

Diese Regel ist jedoch unnötig, falls `FTP_PF_ENABLE_ACTIVE='yes'` benutzt wird – siehe hierzu die Dokumentation des `ftp`-OPTs im `tools`-Paket.

Es folgt eine Übersicht über die existierenden Conntrack-Helfer:

Helfer	Erläuterung
ftp	File Transfer Protocol
h323	H.323 (Voice over IP)
irc	Internet Relay Chat
pptp	PPTP Masquerading (Mit diesem Modul lässt sich mehr als ein PPTP-Client gleichzeitig hinter einem fli4l-Router betreiben.)
sip	Session Initiation Protocol
sane	SANE Network Procotol
snmp	Simple Network Management Protocol
tftp	Trivial File Transfer Protocol

Tabelle 3.8.: Verfügbare Conntrack-Helfer im Paketfilter

Es folgt eine Übersicht der zu konfigurierenden Variablen:

**PF\_PREROUTING\_CT\_ACCEPT\_DEF** Steht diese Variable auf ‘yes’, werden Standard-Regeln generiert, die für ein korrektes Funktionieren des Routers notwendig sind. Standardmäßig sollte man hier ‘yes’ eintragen.

**PF\_PREROUTING\_CT\_N PF\_PREROUTING\_CT\_x PF\_PREROUTING\_CT\_x\_COMMENT**  
Liste der Regeln, die beschreiben, welche eingehenden Pakete vom Router mit Conntrack-Helfern verbunden werden.

**PF\_OUTPUT\_CT\_ACCEPT\_DEF** Steht diese Variable auf ‘yes’, werden Standard-Regeln generiert, die für ein korrektes Funktionieren des Routers notwendig sind. Standardmäßig sollte man hier ‘yes’ eintragen.

**PF\_OUTPUT\_CT\_N PF\_OUTPUT\_CT\_x PF\_OUTPUT\_CT\_x\_COMMENT**  
Liste der Regeln, die beschreiben, welche auf dem Router generierten Pakete vom Router mit Conntrack-Helfern verbunden werden.

### 3.14. Der Paketfilter (IPv6)

Wie für IPv4 wird auch für IPv6-Netzwerke eine Firewall benötigt, damit nicht jeder von außen jeden Rechner im lokalen Netz erreichen kann. Dies ist um so wichtiger, als dass jeder Rechner im Normalfall eine weltweit eindeutige IPv6-Adresse erhält, die dem Rechner permanent zugeordnet werden kann, da sie auf der MAC-Adresse der verwendeten Netzwerkkarte aufbaut.<sup>8</sup> Deshalb verbietet die Firewall erst einmal jegliche Zugriffe von außen und kann dann durch entsprechende Einträge in diesem Abschnitt Stück für Stück – je nach Bedarf – geöffnet werden.

Die Konfiguration der IPv6-Firewall entspricht im Großen und Ganzen der Konfiguration der IPv4-Firewall. Auf Besonderheiten und Unterschiede wird gesondert eingegangen.

<sup>8</sup>Eine Ausnahme existiert, wenn auf den LAN-Hosts die so genannten “Privacy Extensions” aktiviert werden, weil dann ein Teil der IPv6-Adresse zufällig generiert wird. Diese Adressen sind jedoch per Definition nicht nach außen hin bekannt und somit für die Firewall-Konfiguration nur bedingt bis gar nicht relevant.

**PF6\_LOG\_LEVEL** Für alle folgenden Ketten gilt die in PF6\_LOG\_LEVEL vorgenommene Einstellung der Protokoll-Stufe, deren Inhalt auf einen der folgenden Werte gesetzt werden kann: debug, info, notice, warning, err, crit, alert, emerg.

**PF6\_INPUT\_POLICY** Diese Variable legt die Standard-Strategie für auf dem Router eingehende Pakete fest (INPUT-Kette). Mögliche Werte sind "REJECT" (Standard, weist alle Pakete ab), "DROP" (verwirft klammheimlich alle Pakete) und "ACCEPT" (akzeptiert alle Pakete). Für eine genauere Beschreibung siehe die Dokumentation der Variable PF\_INPUT\_POLICY.

Standard-Einstellung: PF6\_INPUT\_POLICY='REJECT'

**PF6\_INPUT\_ACCEPT\_DEF** Diese Variable aktiviert die voreingestellten Regeln für die INPUT-Kette der IPv6-Firewall. Mögliche Werte sind "yes" und "no".

Die voreingestellten Regeln öffnen die Firewall für eingehende ICMPv6-Pings (ein Ping pro Sekunde als Limit) sowie für NDP-Pakete (Neighbour Discovery Protocol), das zur zustandslosen Selbstkonfiguration von IPv6-Netzen benötigt wird. Verbindungen von localhost sowie Antwortpakete zu lokal initiierten Verbindungen werden ebenfalls erlaubt. Schließlich wird die IPv4-Firewall dahingehend angepasst, dass für jeden Tunnel gekapselte IPv6-in-IPv4-Pakete vom Tunnelendpunkt akzeptiert werden.

Standard-Einstellung: PF6\_INPUT\_ACCEPT\_DEF='yes'

**PF6\_INPUT\_LOG** Diese Variable aktiviert das Logging aller zurückgewiesenen eingehenden Pakete. Mögliche Werte sind "yes" und "no". Für eine genauere Beschreibung siehe die Dokumentation der Variable PF\_INPUT\_LOG.

Standard-Einstellung: PF6\_INPUT\_LOG='no'

**PF6\_INPUT\_LOG\_LIMIT** Diese Variable konfiguriert das Log-Limit der INPUT-Kette der IPv6-Firewall, um die Log-Datei lesbar zu halten. Für eine genauere Beschreibung siehe die Dokumentation der Variable PF\_INPUT\_LOG\_LIMIT.

Standard-Einstellung: PF6\_INPUT\_LOG\_LIMIT='3/minute:5'

**PF6\_INPUT\_REJ\_LIMIT** Diese Variable stellt das Limit für das Zurückweisen von eingehenden TCP-Paketen ein. Überschreitet ein solches Paket dieses Limit, wird das Paket klammheimlich verworfen (DROP). Für eine genauere Beschreibung siehe die Dokumentation der Variable PF\_INPUT\_REJ\_LIMIT.

Standard-Einstellung: PF6\_INPUT\_REJ\_LIMIT='1/second:5'

**PF6\_INPUT\_UDP\_REJ\_LIMIT** Diese Variable stellt das Limit für das Zurückweisen von eingehenden UDP-Paketen ein. Überschreitet ein solches UDP-Paket dieses Limit, wird es klammheimlich verworfen (DROP). Für eine genauere Beschreibung siehe die Dokumentation der Variable PF\_INPUT\_UDP\_REJ\_LIMIT.

Standard-Einstellung: PF6\_INPUT\_UDP\_REJ\_LIMIT='1/second:5'

**PF6\_INPUT\_ICMP\_ECHO\_REQ\_LIMIT** Definiert, wie häufig auf eine ICMPv6-Echo-Anfrage reagiert werden soll. Die Häufigkeit wird analog zur Limit-Einschränkung als 'n/Zeiteinheit' mit Bursts beschrieben, also z.B. '3/minute:5'. Ist das Limit überschritten, wird das

### 3. Basiskonfiguration

Paket einfach ignoriert (DROP). Ist dieser Eintrag leer, wird der Standardwert '1/second:5' verwendet; enthält er 'none', wird keine Limitierung durchgeführt.

Standard-Einstellung: `PF6_INPUT_ICMP_ECHO_REQ_LIMIT='1/second:5'`

**PF6\_INPUT\_ICMP\_ECHO\_REQ\_SIZE** Definiert, wie groß eine empfangene ICMPv6-Echo-Anfrage sein darf (in Bytes). In dieser Angabe sind neben den "Nutzdaten" auch die Paket-Header mit zu berücksichtigen. Der Standard-Wert liegt bei 150 Bytes.

Standard-Einstellung: `PF6_INPUT_ICMP_ECHO_REQ_SIZE='150'`

**PF6\_INPUT\_N** Diese Variable enthält die Anzahl der IPv6-Firewallregeln für eingehende Pakete (INPUT-Kette). Standardmäßig werden zwei Regeln aktiviert: Die erste erlaubt allen lokalen Hosts Zugriff auf den Router über so genannte Link-Level-Adressen, und die zweite erlaubt die Kommunikation von Hosts aus dem ersten definierten IPv6-Subnetz mit dem Router.

Falls mehrere lokale IPv6-Subnetze definiert werden, muss die zweite Regel entsprechend oft vervielfältigt werden. Siehe hierzu die Konfigurationsdatei.

Beispiel: `PF6_INPUT_N='2'`

**PF6\_INPUT\_x** Diese Variable spezifiziert eine Regel für die INPUT-Kette der IPv6-Firewall. Für eine genauere Beschreibung siehe die Dokumentation der Variable `PF_INPUT_x`.

Unterschiede zur IPv4-Firewall:

- Anstatt `IP_NET_x` wird hier `IPV6_NET_x` benutzt.
- Anstatt `IP_ROUTE_x` wird hier `IPV6_ROUTE_x` benutzt.
- IPv6-Adressen müssen in eckigen Klammern eingeschlossen werden (inklusive der Netzmaske, falls vorhanden).
- Alle IPv6-Adressangaben (also auch `IPV6_NET_x` etc.) müssen in eckigen Klammern eingeschlossen werden, falls ein Port oder ein Portbereich folgt.

Beispiele:

```
PF6_INPUT_1='[fe80::0/10] ACCEPT'
PF6_INPUT_2='IPV6_NET_1 ACCEPT'
PF6_INPUT_3='tmp1:samba DROP NOLOG'
```

**PF6\_INPUT\_x\_COMMENT** Diese Variable enthält eine Beschreibung bzw. einen Kommentar zur zugehörigen INPUT-Regel.

Beispiel: `PF6_INPUT_3_COMMENT='no_samba_traffic_allowed'`

**PF6\_FORWARD\_POLICY** Diese Variable legt die Standard-Strategie für von dem Router weiterzuleitenden Pakete fest (FORWARD-Kette). Mögliche Werte sind "REJECT" (Standard, weist alle Pakete ab), "DROP" (verwirft klammheimlich alle Pakete) und "ACCEPT" (akzeptiert alle Pakete). Für eine genauere Beschreibung siehe die Dokumentation der Variable `PF_FORWARD_POLICY`.

Standard-Einstellung: `PF6_FORWARD_POLICY='REJECT'`

**PF6\_FORWARD\_ACCEPT\_DEF** Diese Variable aktiviert die voreingestellten Regeln für die FORWARD-Kette der IPv6-Firewall. Mögliche Werte sind “yes” und “no”.

Die voreingestellten Regeln öffnen die Firewall für ausgehende ICMPv6-Pings (ein Ping pro Sekunde als Limit). Antwortpakete zu bereits erlaubten Verbindungen werden ebenfalls erlaubt.

Standard-Einstellung: `PF6_FORWARD_ACCEPT_DEF='yes'`

**PF6\_FORWARD\_LOG** Diese Variable aktiviert das Logging aller zurückgewiesenen weiterzuleitenden Pakete. Mögliche Werte sind “yes” und “no”. Für eine genauere Beschreibung siehe die Dokumentation der Variable `PF_FORWARD_LOG`.

Standard-Einstellung: `PF6_FORWARD_LOG='no'`

**PF6\_FORWARD\_LOG\_LIMIT** Diese Variable konfiguriert das Log-Limit der FORWARD-Kette der IPv6-Firewall, um die Log-Datei lesbar zu halten. Für eine genauere Beschreibung siehe die Dokumentation der Variable `PF_FORWARD_LOG_LIMIT`.

Standard-Einstellung: `PF6_FORWARD_LOG_LIMIT='3/minute:5'`

**PF6\_FORWARD\_REJ\_LIMIT** Diese Variable stellt das Limit für das Zurückweisen von weiterzuleitenden TCP-Paketen ein. Überschreitet ein solches TCP-Paket dieses Limit, wird es klammheimlich verworfen (DROP). Für eine genauere Beschreibung siehe die Dokumentation der Variable `PF_FORWARD_REJ_LIMIT`.

Standard-Einstellung: `PF6_FORWARD_REJ_LIMIT='1/second:5'`

**PF6\_FORWARD\_UDP\_REJ\_LIMIT** Diese Variable stellt das Limit für das Zurückweisen von weiterzuleitenden UDP-Paketen ein. Überschreitet ein solches UDP-Paket dieses Limit, wird es klammheimlich verworfen (DROP). Für eine genauere Beschreibung siehe die Dokumentation der Variable `PF_FORWARD_UDP_REJ_LIMIT`.

Standard-Einstellung: `PF6_FORWARD_UDP_REJ_LIMIT='1/second:5'`

**PF6\_FORWARD\_N** Diese Variable enthält die Anzahl der IPv6-Firewallregeln für weiterzuleitende Pakete (FORWARD-Kette). Standardmäßig werden zwei Regeln aktiviert: Die erste verhindert die Weiterleitung aller lokalen Samba-Pakete in nicht-lokale Netze, und die zweite erlaubt letzteres für alle anderen lokalen Pakete aus dem ersten definierten IPv6-Subnetz.

Falls mehrere lokale IPv6-Subnetze definiert werden, muss die letzte Regel entsprechend oft vervielfältigt werden. Siehe hierzu die Konfigurationsdatei.

Beispiel: `PF6_FORWARD_N='2'`

**PF6\_FORWARD\_x** Diese Variable spezifiziert eine Regel für die FORWARD-Kette der IPv6-Firewall. Für eine genauere Beschreibung siehe die Dokumentation der Variable `PF_FORWARD_x`.

Unterschiede zur IPv4-Firewall:

- Anstatt `IP_NET_x` wird hier `IPV6_NET_x` benutzt.
- Anstatt `IP_ROUTE_x` wird hier `IPV6_ROUTE_x` benutzt.
- IPv6-Adressen müssen in eckigen Klammern eingeschlossen werden (inklusive der Netzmaske, falls vorhanden).

### 3. Basiskonfiguration

- Alle IPv6-Adressangaben (also auch IPV6\_NET\_x etc.) müssen in eckigen Klammern eingeschlossen werden, falls ein Port oder ein Portbereich folgt.

Beispiele:

```
PF6_FORWARD_1='tmpl:samba DROP'  
PF6_FORWARD_2='IPV6_NET_1 ACCEPT'
```

**PF6\_FORWARD\_x\_COMMENT** Diese Variable enthält eine Beschreibung bzw. einen Kommentar zur zugehörigen FORWARD-Regel.

Beispiel: PF6\_FORWARD\_1\_COMMENT='no\_samba\_traffic\_allowed'

**PF6\_OUTPUT\_POLICY** Diese Variable legt die Standard-Strategie für vom Router ausgehende Pakete fest (OUTPUT-Kette). Mögliche Werte sind "REJECT" (Standard, weist alle Pakete ab), "DROP" (verwirft klammheimlich alle Pakete) und "ACCEPT" (akzeptiert alle Pakete). Für eine genauere Beschreibung siehe die Dokumentation der Variable PF\_OUTPUT\_POLICY.

Standard-Einstellung: PF6\_OUTPUT\_POLICY='REJECT'

**PF6\_OUTPUT\_ACCEPT\_DEF** Diese Variable aktiviert die voreingestellten Regeln für die OUTPUT-Kette der IPv6-Firewall. Mögliche Werte sind "yes" und "no". Momentan existieren keine voreingestellten Regeln.

Standard-Einstellung: PF6\_OUTPUT\_ACCEPT\_DEF='yes'

**PF6\_OUTPUT\_LOG** Diese Variable aktiviert das Logging aller zurückgewiesenen ausgehenden Pakete. Mögliche Werte sind "yes" und "no". Für eine genauere Beschreibung siehe die Dokumentation der Variable PF\_OUTPUT\_LOG.

Standard-Einstellung: PF6\_OUTPUT\_LOG='no'

**PF6\_OUTPUT\_LOG\_LIMIT** Diese Variable konfiguriert das Log-Limit der OUTPUT-Kette der IPv6-Firewall, um die Log-Datei lesbar zu halten. Für eine genauere Beschreibung siehe die Dokumentation der Variable PF\_OUTPUT\_LOG\_LIMIT.

Standard-Einstellung: PF6\_OUTPUT\_LOG\_LIMIT='3/minute:5'

**PF6\_OUTPUT\_REJ\_LIMIT** Diese Variable stellt das Limit für das Zurückweisen von ausgehenden TCP-Paketen ein. Überschreitet ein solches Paket dieses Limit, wird das Paket klammheimlich verworfen (DROP). Für eine genauere Beschreibung siehe die Dokumentation der Variable PF\_OUTPUT\_REJ\_LIMIT.

Standard-Einstellung: PF6\_OUTPUT\_REJ\_LIMIT='1/second:5'

**PF6\_OUTPUT\_UDP\_REJ\_LIMIT** Diese Variable stellt das Limit für das Zurückweisen von ausgehenden UDP-Paketen ein. Überschreitet ein solches UDP-Paket dieses Limit, wird es klammheimlich verworfen (DROP). Für eine genauere Beschreibung siehe die Dokumentation der Variable PF\_OUTPUT\_UDP\_REJ\_LIMIT.

Standard-Einstellung: PF6\_OUTPUT\_UDP\_REJ\_LIMIT='1/second:5'



**PF6\_OUTPUT\_N** Diese Variable enthält die Anzahl der IPv6-Firewallregeln für eingehende Pakete (OUTPUT-Kette). Standardmäßig werden zwei Regeln aktiviert: Die erste erlaubt allen lokalen Hosts Zugriff auf den Router über so genannte Link-Level-Adressen, und die zweite erlaubt die Kommunikation von Hosts aus dem ersten definierten IPv6-Subnetz mit dem Router.

Falls mehrere lokale IPv6-Subnetze definiert werden, muss die zweite Regel entsprechend oft vervielfältigt werden. Siehe hierzu die Konfigurationsdatei.

Beispiel: `PF6_OUTPUT_N='1'`

**PF6\_OUTPUT\_x** Diese Variable spezifiziert eine Regel für die OUTPUT-Kette der IPv6-Firewall. Für eine genauere Beschreibung siehe die Dokumentation der Variable `PF_OUTPUT_x`.

Unterschiede zur IPv4-Firewall:

- Anstatt `IP_NET_x` wird hier `IPV6_NET_x` benutzt.
- Anstatt `IP_ROUTE_x` wird hier `IPV6_ROUTE_x` benutzt.
- IPv6-Adressen müssen in eckigen Klammern eingeschlossen werden (inklusive der Netzmaske, falls vorhanden).
- Alle IPv6-Adressangaben (also auch `IPV6_NET_x` etc.) müssen in eckigen Klammern eingeschlossen werden, falls ein Port oder ein Portbereich folgt.

Beispiele:

```
PF6_OUTPUT_1='tmpl:ftp IPV6_NET_1 ACCEPT HELPER:ftp'
```

**PF6\_OUTPUT\_x\_COMMENT** Diese Variable enthält eine Beschreibung bzw. einen Kommentar zur zugehörigen OUTPUT-Regel.

Beispiel: `PF6_OUTPUT_3_COMMENT='no_samba_traffic_allowed'`

**PF6\_USR\_CHAIN\_N** Diese Variable enthält die Anzahl der vom Benutzer definierten IPv6-Firewall-Tabellen. Für eine genauere Beschreibung siehe die Dokumentation der Variable `PF_USR_CHAIN_N`.

Standard-Einstellung: `PF6_USR_CHAIN_N='0'`

**PF6\_USR\_CHAIN\_x\_NAME** Diese Variable enthält den Namen der entsprechenden benutzerdefinierten IPv6-Firewall-Tabelle. Für eine genauere Beschreibung siehe die Dokumentation der Variable `PF_USR_CHAIN_x_NAME`.

Beispiel: `PF6_USR_CHAIN_1_NAME='usr-myvpn'`

**PF6\_USR\_CHAIN\_x\_RULE\_N** Diese Variable enthält die Anzahl der IPv6-Firewallregeln in der zugehörigen benutzerdefinierten IPv6-Firewall-Tabelle. Für eine genauere Beschreibung siehe die Dokumentation der Variable `PF_USR_CHAIN_x_RULE_N`.

Beispiel: `PF6_USR_CHAIN_1_RULE_N='0'`

**PF6\_USR\_CHAIN\_x\_RULE\_x** Diese Variable spezifiziert eine Regel für die benutzerdefinierte IPv6-Firewall-Tabelle. Für eine genauere Beschreibung siehe die Dokumentation der Variable `PF_USR_CHAIN_x_RULE_x`.

Unterschiede zur IPv4-Firewall:

- Anstatt `IP_NET_x` wird hier `IPV6_NET_x` benutzt.
- Anstatt `IP_ROUTE_x` wird hier `IPV6_ROUTE_x` benutzt.
- IPv6-Adressen müssen in eckigen Klammern eingeschlossen werden (inklusive der Netzmaske, falls vorhanden).
- Alle IPv6-Adressangaben (also auch `IPV6_NET_x` etc.) müssen in eckigen Klammern eingeschlossen werden, falls ein Port oder ein Portbereich folgt.

**PF6\_USR\_CHAIN\_x\_RULE\_x\_COMMENT** Diese Variable enthält eine Beschreibung bzw. einen Kommentar zur zugehörigen Regel.

Beispiel: `PF6_USR_CHAIN_1_RULE_1_COMMENT='some_user-defined_rule'`

**PF6\_POSTROUTING\_N** Diese Variable enthält die Anzahl der IPv6-Firewallregeln fürs Maskieren (POSTROUTING-Kette). Für eine genauere Beschreibung siehe die Dokumentation der Variable `PF_POSTROUTING_N`.

Beispiel: `PF6_POSTROUTING_N='2'`

**PF6\_POSTROUTING\_x PF6\_POSTROUTING\_x\_COMMENT**

Eine Liste der Regeln, die beschreiben, welche IPv6-Pakete vom Router maskiert werden (bzw. unmaskiert weitergeleitet werden). Für eine genauere Beschreibung siehe die Dokumentation der Variable `PF_POSTROUTING_x`.

**PF6\_PREROUTING\_N** Diese Variable enthält die Anzahl der IPv6-Firewallregeln fürs Weiterleiten an ein anderes Ziel (PREROUTING-Kette). Für eine genauere Beschreibung siehe die Dokumentation der Variable `PF_PREROUTING_N`.

Beispiel: `PF6_PREROUTING_N='2'`

**PF6\_PREROUTING\_x PF6\_PREROUTING\_x\_COMMENT**

Eine Liste der Regeln, die beschreiben, welche IPv6-Pakete vom Router an ein anderes Ziel weitergeleitet werden sollen. Für eine genauere Beschreibung siehe die Dokumentation der Variable `PF_PREROUTING_x`.

## 3.15. Domain-Konfiguration

Windows-PCs im LAN haben eine unangenehme Eigenschaft: Sobald ein Nameserver benötigt wird und man diesen deshalb im Windows einstellt, fragen diese Windows-Rechner den angegebenen Nameserver in regelmäßigen Abständen ab – auch wenn man gar nicht daran arbeitet! Würde man also auf dem Windows-PC einen DNS-Server im Internet angeben, wird's teuer...

Der Trick ist nun folgender: Wenn im LAN nicht bereits ein DNS-Server vorhanden ist, kann man den DNS-Server im fli4l-Router verwenden.

Es wird DNSMASQ als DNS-Server eingesetzt.

Wenn man jedoch mit der DNS-Konfiguration beginnt, sollte man sich zunächst Gedanken über den Domain-Namen und die Namen der PCs im Netz machen. Der verwendete Domain-Name wird nicht im Internet sichtbar. Deshalb kann man sich hier prinzipiell beliebige Domain-Namen ausdenken.

Außerdem sollte man jedem Windows-Rechner einen Namen verpassen. Diese Namen müssen dem fli4l-Router bekannt sein.

**DOMAIN\_NAME** Standard-Einstellung: `DOMAIN_NAME='lan.fli4l'`

Hier kann sich jeder austoben, da die lokal verwendete Domain nicht im Internet sichtbar wird. Sie sollten lediglich vermeiden, einen Namen zu benutzen, den es im Internet geben könnte (z.B. `irgendwas.de`), da Sie sonst nicht auf diese Domain werden zugreifen können.

**DNS\_FORWARDERS** Standard-Einstellung: `DNS_FORWARDERS=""`

Hier ist die DNS-Server-Adresse des Internet-Providers anzugeben, wenn fli4l als Router in das Internet verwendet wird. Der fli4l-Router gibt dann sämtliche DNS-Anfragen, die er nicht selbst beantworten kann, an diese Adresse weiter.

Möchte man mehrere DNS-Forwarder angeben, trennt man die IP-Adressen durch Leerzeichen.

Sind mehrere DNS-Server konfiguriert werden diese in der angegebenen Reihenfolge für DNS-Anfragen genutzt, somit wird der zweite angegebene Server nur genutzt, wenn der erste keine Antwort liefert usw.

Es ist auch möglich, optional Port-Nummern an die IP-Adressen durch Doppelpunkt getrennt anzugeben. Allerdings muss dann `OPT_DNS='yes'` (Seite 132) sein (Paket `dns_dhcp` (Seite 131)) und es darf nirgends die Option `*_USEPEERDNS` benutzt werden.

Achtung: Auch wenn

- `PPPOE_USEPEERDNS` (Seite ??),
- `ISDN_CIRC_x_USEPEERDNS` (Seite 184) oder
- `DHCP_CLIENT_x_USEPEERDNS` (Seite ??)

gesetzt (`=yes`) ist, ist hier die Eintragung eines Servers nötig, da sonst direkt nach dem Start keine Namensauflösung möglich ist.

Ausnahme: fli4l als Router in einem lokalen Netz *ohne* Anschluss an das Internet oder (Firmen-)Netze mit weiteren DNS-Servern. In diesem Fall ist `127.0.0.1` anzugeben, um das Weiterleiten zu unterbinden.

**HOSTNAME\_IP** (optional)

Hiermit kann optional festgelegt werden, an welches Netz `IP_NET_x` der `HOSTNAME` gebunden wird.

**HOSTNAME\_ALIAS\_N** (optional)

Anzahl der zusätzlichen Alias-Hostnamen für den Router.

**HOSTNAME\_ALIAS\_x** (optional)

Zusätzlicher Alias-Name für den Router.

## 3.16. imond-Konfiguration

**OPT\_IMOND** Standard-Einstellung: `OPT_IMOND='no'`

Mit `OPT_IMOND` kann man einstellen, ob der imond-Server aktiviert werden soll. imond übernimmt dabei das Monitoring/Controlling und Least-Cost-Routing des fli4l-Routers. Der [Beschreibung von imond](#) (Seite 319) ist deshalb ein extra Kapitel gewidmet (s.u.).

### 3. Basiskonfiguration

Wichtig: Die LC-Routing-Features von fli4l können nur mit imond genutzt werden. Ein zeitabhängiges Umschalten von Verbindungen ist ohne imond nicht möglich!

Für ISDN- und DSL-Routing ist imond ab Version 1.5 zwingend erforderlich. In diesem Fall ist `OPT_IMOND='yes'` einzustellen.

Wird fli4l lediglich als Router zwischen 2 Netzwerken eingesetzt, sollte `OPT_IMOND='no'` eingestellt werden.

**IMOND\_PORT** TCP/IP-Port, auf dem imond auf Verbindungen horcht. Der Standard-Wert '5000' sollte nur in Ausnahmefällen geändert werden.

**IMOND\_PASS** Standard-Einstellung: `IMOND_PASS=""`

Hier kann ein spezielles User-Password für imond gesetzt werden. Meldet sich ein Client auf Port 5000 an, erwartet imond (und damit auch seine Clients) die Eingabe dieses Passwords, bevor er irgendeinen Befehl korrekt beantwortet. Ausnahme: Befehle "quit", "help" und "pass". Ist `IMOND_PASS` leer, wird kein Password benötigt.

Ob der Client im User-Modus bestimmte Steuerbefehle, wie Dial, Hangup, Reboot, Umschalten der Default-Route bereits ausführen kann oder dafür die Eingabe des Admin-Passwords zwingend notwendig ist, wird über die Variablen

- [IMOND\\_ENABLE](#) (Seite 86),
- [IMOND\\_DIAL](#) (Seite 85),
- [IMOND\\_ROUTE](#) (Seite 85) und
- [IMOND\\_REBOOT](#) (Seite 85)

eingestellt, siehe unten.

**IMOND\_ADMIN\_PASS** Standard-Einstellung: `IMOND_ADMIN_PASS=""`

Mit Hilfe der Admin-Passwords erhält der Client alle Rechte und kann so sämtliche Steuerfunktionen des imond-Servers nutzen – und zwar unabhängig von den Variablen `IMOND_ENABLE`, `IMOND_DIAL` usw. Lässt man `IMOND_ADMIN_PASS` leer, so reicht die Eingabe des User-Passwords, um sämtliche Rechte zu erhalten!

**IMOND\_LED** imond kann den Online/Offline-Status nun über eine LED anzeigen. Diese wird folgendermaßen an einen COM-Port angeschlossen:

Verbindung 25-polig:

```
20 DTR  ----- 1kOhm ----- >| ----- 7 GND
```

Verbindung 9-polig:

```
4 DTR  ----- 1kOhm ----- >| ----- 5 GND
```

Ist eine ISDN- oder DSL-Verbindung aufgebaut, leuchtet die LED. Ansonsten ist sie ausgeschaltet. Sollte es genau umgekehrt sein, ist die Leuchtdiode umzupolen. Sollte die LED zu schwach leuchten, kann der Vorwiderstand bis auf 470 Ohm reduziert werden.

Es ist auch möglich, zwei verschiedenfarbige LEDs anzuschließen. Dann ist die zweite LED ebenso über einen Vorwiderstand zwischen DTR und GND anzuschließen, jedoch

### 3. Basiskonfiguration

genau umgekehrt. Dann leuchtet je nach Zustand die eine oder die andere LED. Oder man verwendet direkt eine DUO-LED (zweifarbige, drei Anschlussbeinchen).

Im Moment verhält sich der RTS-Anschluss der seriellen Schnittstelle genauso wie DTR. Hier könnte also noch eine weitere LED angeschlossen werden, die den Online/Offline-Zustand anzeigt. Das könnte sich jedoch in einer zukünftigen fli4l-Version ändern.

Als Wert von `IMOND_LED` muss ein COM-Port angegeben werden, also `'com1'`, `'com2'`, `'com3'` oder `'com4'`. Ist keine LED angeschlossen, sollte die Variable leer gelassen werden.

**IMOND\_BEEP** Mit `IMOND_BEEP='yes'` gibt imond einen Zweiklang-Ton über den PC-Lautsprecher aus, wenn der Zustand von Offline nach Online wechselt und umgekehrt. Im ersten Fall wird zuerst ein tiefer, dann ein hoher Ton ausgegeben. Beim Wechsel in den Offline-Status zurück wird zuerst der höhere, dann der tiefere Ton ausgegeben.

**IMOND\_LOG** Standard-Einstellung: `IMOND_LOG='no'`

Wird `IMOND_LOG='yes'` benutzt, werden in der Datei `/var/log/imond.log` die Verbindungen protokolliert. Diese Datei kann z.B. für Statistikzwecke per scp auf einen Rechner im LAN kopiert werden. Für den scp-Zugriff ist aber dann noch das Paket sshd zu installieren und so zu konfigurieren, dass es auch scp zur Verfügung stellt.

Das Format der Logdateieinträge ist in Tabelle 3.9 beschrieben.

Tabelle 3.9.: Format der Imond-Logdatei

Eintrag	Bedeutung
Circuit	der Name des Circuits, für den der Eintrag erzeugt wurde
Startzeit	Datum und Uhrzeit der Einwahl dieses Circuits
Stopzeit	Datum und Uhrzeit des Auflegens dieses Circuits
Online-Zeit	die Zeit, die dieser Circuit online war
Abgerechnete Zeit	die Zeit, die der Provider abrechnen wird (hängt vom Takt ab)
Kosten	die Kosten, die der Provider für die Zeit in Rechnung stellt
Bandbreite	die genutzte Bandbreite getrennt nach in und out (in zuerst), dargestellt als zwei vorzeichenlose Integerzahlen, für die gilt: Bandbreite = $4\text{GiB} * <\text{erste Zahl}> + <\text{zweite Zahl}>$
Device	das Gerät, über das kommuniziert wurde
Abrechnungstakt	der Takt, der vom Provider zur Abrechnung herangezogen wird (Daten der Circuit-Konfiguration)
Taktgebühren	die Gebühren, die pro Takt fällig werden (Daten der Circuit-Konfiguration)

Die Kosten werden in Euro ausgegeben. Wichtig ist dabei die korrekte Definition der entsprechenden Circuit-Variablen `ISDN_CIRC_x_TIMES` (Seite 191).

**IMOND\_LOGDIR** Ist das Protokollieren eingeschaltet, kann über `IMOND_LOGDIR` ein alternatives Verzeichnis statt `/var/log` angegeben werden, z.B. `'/boot'`. Dann wird die Log-Datei `imond.log` auf dem Bootmedium angelegt. Dazu muss dieses aber auch Read/Write „gemounted“ sein. Default ist `'auto'` was den Speicherort automatisch bestimmt. Je nach weiterer Konfiguration liegt das dann unter `/boot/persistent/base` oder an einem anderen durch `FLI4L_UUID` bestimmten Pfad. Ist `/boot` nicht Read/Write und `FLI4L_UUID` nicht gesetzt, befindet sich das File unter `/var/run`.

**IMOND\_ENABLE IMOND\_DIAL IMOND\_ROUTE IMOND\_REBOOT** Durch diese Variablen werden bestimmte Kommandos, die von imonc-Clients zum imond-Server gesendet werden, bereits im User-Modus freigeschaltet.

Hiermit kann man einstellen, ob der imond-Server die ISDN-Schnittstelle ein- bzw. ausschalten, wählen/einhängen, eine neue Default-Route setzen und/oder den Rechner booten darf.

Standard-Einstellungen:

```
IMOND_ENABLE='yes'
IMOND_DIAL='yes'
IMOND_ROUTE='yes'
IMOND_REBOOT='yes'
```

Alle weiteren Features der Client-/Server-Schnittstelle von imond sind in einem [eigenen Kapitel](#) (Seite [319](#)) beschrieben.

## 3.17. Circuit-Konfiguration

### 3.17.1. Circuits allgemein

Der fli4l-Router erlaubt ab Version 4.0, Verbindungen nach “außen” flexibel über so genannte “Circuits” zu konfigurieren. Der Begriff “Circuit” kommt aus dem Englischen und bedeutet in diesem Zusammenhang so viel wie “Leitung”. Seine Verwendung in fli4l entstammt dem Wählen und Auflegen von ISDN-Verbindungen, das seit der ersten fli4l-Version möglich ist; da ISDN ein leitungsvermittelnder (“circuit-switched”) Dienst ist, hat sich der Begriff etabliert und wird heute in allen anderen Verbindungs-Situationen verwendet, auch wenn es meistens nicht mehr um leitungsvermittelnde, sondern um paketvermittelnde Dienste geht. Auch in dieser Dokumentation wird der Begriff des Circuits durchgängig verwendet.

Ein konfigurierter Circuit erlaubt es dem fli4l-Router, irgendeine Form der Verbindung zwischen dem Router und einem anderen Netzwerk-Kommunikationspartner herzustellen. Meistens, aber nicht immer, geht es dabei um die Herstellung einer Internet-Anbindung. Im Folgenden wird eine kurze Übersicht darüber gegeben, welche Circuit-Typen der fli4l-Router beherrscht (die meisten davon werden jedoch von anderen Paketen angeboten, dies ist aber entsprechend in der Tabelle vermerkt).

Typ	Paket	OPT	Beschreibung
route	base	-	Mit Hilfe von route-Circuits können Routen in andere Netze konfiguriert werden. Dies entspricht im Wesentlichen der Funktionalität der Variablen IP_ROUTE_% (siehe <a href="#">IP_ROUTE_N</a> (Seite <a href="#">48</a> )), geht jedoch etwas darüber hinaus. Intern werden alle per IP_ROUTE_% konfigurierte Routen in route-Circuits abgebildet.

### 3. Basiskonfiguration

Typ	Paket	OPT	Beschreibung
dhcp	dhcp_client	OPT_DHCP_CLIENT	Mit Hilfe von dhcp-Circuits lassen sich IPv4- und IPv6-Adressinformationen von einem DHCP-Server ermitteln. Dies ist vor allem dann sinnvoll, wenn der fii4l nicht selbsttätig eine Internet-Verbindung aufbaut, sondern sich hinter einem anderen Router befindet, der dies für einen erledigt, etwa hinter einem Kabelmodem.
isdn	isdn	OPT_ISDN	Mit Hilfe von isdn-Circuits ist eine Einwahl in ein anderes Netz (z. B. ein Firmennetz) über ISDN möglich.
ppp	ppp (+ diverse)	OPT_PPP (+ diverse)	Mit Hilfe von ppp-Circuits ist eine Einwahl ins Internet oder ein Firmennetz über eine Reihe diverser Kanäle mit Hilfe des Point-to-Point-Protokolls (PPP) möglich. Mehr dazu ist in Abschnitt <a href="#">4.17.1</a> zu finden.

Tabelle 3.10.: Verfügbare Circuit-Typen

Alle Circuits werden der Übersichtlichkeit halber in der Datei `circuits.txt` konfiguriert. Die Anzahl der konfigurierten Circuits wird dabei in der Variable `CIRC_N` festgehalten:

**CIRC\_N** Diese Variable gibt die Anzahl der konfigurierten Circuits an.

Standard-Einstellung: `CIRC_N='0'`

Beispiel: `CIRC_N='4'`

Darüber hinaus besitzt jeder Circuit, egal von welchem Typ, einige allgemeine Attribute. Zuerst operiert *jeder* Circuit auf einer *Netzwerk-Schnittstelle*. Je nach Circuit-Typ ist diese Schnittstelle statisch vorhanden (dies gilt z. B. für Ethernet-Schnittstellen wie “eth0”), oder sie wird dynamisch beim Einwählen erzeugt (das ist z. B. bei den “pppX”-Schnittstellen von ppp-Circuits der Fall), oder sie wird von einem anderen Circuit erzeugt und hier nur referenziert (das ist z. B. bei DHCPv6-over-PPPoE der Fall). Auf Grund dieser verschiedenen Möglichkeiten gibt es keine einheitliche Variable zur Angabe der Schnittstelle, stattdessen kümmert sich jeder Circuit-Typ selbst um die Konfiguration der Schnittstelle (und einige wie ppp verbieten die Angabe einer Schnittstelle gänzlich, da sie automatisch erzeugt und verwaltet wird).

Weitere allgemeine Attribute werden über die folgenden Variablen konfiguriert.

**CIRC\_x\_NAME** Jeder Circuit hat einen Namen. Dieser Name kann aus Buchstaben, Ziffern und dem Bindestrich (‘-’) bestehen und hilft dabei, den Circuit in der Web-GUI, in Protokollen etc. zu identifizieren. Der Name muss unter allen Circuits und Circuit-Klassen (siehe [CIRC\\_CLASS\\_x\\_NAME](#) (Seite 97)) eindeutig sein.

Beispiel: `CIRC_x_NAME='DSL-Telekom'`

**CIRC\_x\_TYPE** Jeder Circuit hat einen Typ. Dieser Typ bestimmt, wie das Wählen und Auflegen funktioniert. Intern entscheidet der Typ, welches Skript zum Wählen und Auflegen verwendet wird.

Es sind immer nur die Typen der aktivierten Pakete verfügbar. Wenn Sie also z. B. einen dhcp-Circuit verwenden möchten, dann müssen Sie das Paket `dhcp_client` herunterladen und DHCP mit `OPT_DHCP_CLIENT='yes'` aktivieren. Andernfalls bekommen Sie bei der Verwendung des Typs "dhcp" beim Bauen der Installationsarchive eine Fehlermeldung.

Beispiel: `CIRC_x_TYPE='dhcp'`

**CIRC\_x\_ENABLED** Die Variable `CIRC_x_ENABLED` aktiviert einen Circuit zur Konfigurationszeit. Damit der Circuit überhaupt Beachtung findet, muss diese Variable auf `'yes'` gesetzt werden. Gilt hingegen `CIRC_x_ENABLED='no'`, dann wird der Circuit auf dem fl4l nicht konfiguriert. Auch kann zur Konfigurationszeit der Circuits nicht mit seinem Namen angesprochen werden, etwa in Firewall-Regeln.

Standard-Einstellung: `CIRC_x_ENABLED='no'`

Beispiel: `CIRC_x_ENABLED='yes'`

**CIRC\_x\_DIALMODE** Jeder Circuit kann einen individuellen initialen [Wählmodus](#) (Seite 95) erhalten, der dann über diese Variable konfiguriert werden kann.

Standard-Einstellung: `CIRC_x_DIALMODE='auto'`

Beispiel: `CIRC_x_DIALMODE='manual'`

**CIRC\_x\_NETS\_IPV4\_y** Ein Circuit ist nur dann sinnvoll, wenn er auch zu einer Netzanbindung führt. Dazu ist es in der Regel notwendig, dass Routen konfiguriert werden, sobald eine erfolgreiche Einwahl stattgefunden hat. Welche IPv4-Netze über den Circuit geroutet werden, kann über diese Variablen festgelegt werden.

Im häufigsten Fall der Circuit-Nutzung, der Internet-Anbindung, muss die Default-Route über den Circuit gehen. Dazu muss das Netz `0.0.0.0/0` in die Liste eingetragen werden.

Nur in Ausnahmefällen müssen keine Netze angegeben werden, etwa bei Server-Circuits, bei denen keine Routen zurück zu den Clients installiert werden sollen.

Standard-Einstellung: `CIRC_x_NETS_IPV4_N='0'`

Beispiel 1:

```
CIRC_x_NETS_IPV4_N='1'
CIRC_x_NETS_IPV4_1='0.0.0.0/0'
```

Beispiel 2:

```
CIRC_x_NETS_IPV4_N='2'
CIRC_x_NETS_IPV4_1='10.15.16.0/24'
CIRC_x_NETS_IPV4_2='10.16.0.0/16'
```

**CIRC\_x\_NETS\_IPV6\_y** Hier werden analog zu `CIRC_x_NETS_IPV4_y` IPv6-Netze angegeben, die nach der Einwahl über den Circuit geroutet werden sollen. Diese Variablen können nur bei aktivierter IPv6-Unterstützung (Paket `ipv6`, `OPT_IPV6='yes'`) verwendet werden.



### 3. Basiskonfiguration

Im häufigsten Fall der Circuit-Nutzung, der Internet-Anbindung, muss die Default-Route über den Circuit gehen. Dazu muss das Netz `::/0` in die Liste eingetragen werden.

Nur in Ausnahmefällen müssen keine Netze angegeben werden, etwa bei Server-Circuits, bei denen keine Routen zurück zu den Clients installiert werden sollen.

Standard-Einstellung: `CIRC_x_NETS_IPV6_N='0'`

Beispiel 1:

```
CIRC_x_NETS_IPV6_N='1'
CIRC_x_NETS_IPV6_1='::/0'
```

Beispiel 2:

```
CIRC_x_NETS_IPV6_N='2'
CIRC_x_NETS_IPV6_1='2001:db8:1::/48'
CIRC_x_NETS_IPV6_2='2001:db8:2::/48'
```

**CIRC\_x\_PROTOCOLS** In der Regel werden die Layer-3-Protokolle, die von einem Circuit unterstützt werden (IPv4 oder IPv6) aus den konfigurierten Netzen (`CIRC_x_NETS_IPV4_y` und `CIRC_x_NETS_IPV6_y`, siehe oben) abgeleitet. In manchen Fällen werden jedoch keine Netze angegeben, weil keine Routen aufgebaut werden sollen. Dies ist beispielsweise bei Server-Circuits der Fall. In solchen Fällen ist es nötig, die zu verwendenden Layer-3-Protokolle explizit einzustellen. Dazu wird in dieser Variable eine Liste von Protokollen notiert, die durch Leerzeichen voneinander getrennt sind. Erlaubte Protokolle sind `ipv4` und `ipv6`.

Standard-Einstellung: abgeleitet aus `CIRC_x_NETS_IPV4_y` und `CIRC_x_NETS_IPV6_y`

Beispiel: `CIRC_x_PROTOCOLS='ipv4 ipv6'`

**CIRC\_x\_UP** Ist `CIRC_x_UP='yes'`, dann wird der entsprechende Circuit beim Booten aktiviert. Je nach [Wählmodus](#) (Seite 95) kann dies bereits beim Booten zu einer Einwahl führen, oder die Einwahl kann später über die GUI oder das `fli4lctrl`-Programm veranlasst werden. Bei `CIRC_x_UP='no'` muss der Circuit erst mit Hilfe der GUI oder mit dem `fli4lctrl`-Programm aktiviert werden, bevor eine Einwahl gestartet werden kann. Falls Circuits aktiviert werden, die sich in einem oder mehreren gerouteten Netzen überlappen, ist dies ein Fehler, der bereits beim Versuch, das Installationsarchiv zu bauen, von `mkfli4l` gemeldet wird.<sup>9</sup>

Diese Einstellung ist nur relevant mit `OPT_CIRCD='no'`.

Standard-Einstellung: `CIRC_x_UP='no'`

Beispiel: `CIRC_x_UP='yes'`

**CIRC\_x\_PRIORITY** Diese Variable gibt die Priorität des Circuits an. Höhere Werte bedeuten eine niedrigere Priorität. Prioritäten dienen dazu, Circuits nach Eignung zu gruppieren: Bei der Auswahl von Circuits<sup>10</sup> werden alle Circuits prioritätsweise abgearbeitet. Nur

---

<sup>9</sup>In einer späteren Version ist angedacht, in einem solchen Fall den Datenverkehr für diese Netze gleichmäßig auf alle diese Circuits zu verteilen.

<sup>10</sup>durch den Hintergrundprozess `circd`

### 3. Basiskonfiguration

wenn in der höchsten Prioritätsklasse keine Circuits in Frage kommen, kommen die Circuits der nächstniedrigeren Prioritätsklasse zum Zuge. Mehr zum Auswahlalgorithmus des `cird` finden Sie im Abschnitt [“Das Programm `circd`”](#) (Seite 100).

Diese Einstellung ist nur relevant mit `OPT_CIRCD='yes'`.

Standard-Einstellung: `CIRC_x_PRIORITY='1'`

Beispiel: `CIRC_x_PRIORITY='2'`

**CIRC\_x\_TIMES** Ist `OPT_CIRCD='yes'`, dann enthält diese Variable eine Zeitspezifikation, die angibt, wann der Circuit aktiviert werden soll und wann nicht, und wie viel der Circuit bei einer erfolgreichen Einwahl pro Minute kostet. Dadurch wird es möglich, zu verschiedenen Zeiten verschiedene Circuits zu verwenden (Least-Cost-Routing). Dabei kontrolliert der Dämon-Prozess `circd` das Aktivieren und Deaktivieren der Circuits.

Der Inhalt der Variablen ist wie folgt aufgebaut:

```
CIRC_x_TIMES='W1-W2:hh-hh:Kosten:Typ [W1-W2:hh-hh:Kosten:Typ [...]]'
```

Jedes Feld besteht aus vier Unterfeldern, die mit Hilfe eines Doppelpunkts (':') voneinander getrennt sind:

- Feld *W1-W2*: Wochentag-Zeitraum, z. B. Mo-Fr oder Sa-Su usw. Sowohl die deutsche als auch die englische Schreibweise sind erlaubt. Soll ein einzelner Wochentag eingetragen werden, ist W1-W1 zu schreiben, also z. B. Su-Su.
- Feld *hh-hh*: Stunden-Bereich, z. B. 09-18 oder auch 18-09. 18-09 ist gleichbedeutend mit 18-24 plus 00-09. 00-24 meint den ganzen Tag. Stunden müssen immer zweistellig (also notfalls mit führenden Nullen) angegeben werden.
- Feld *Kosten*: Hier werden in Euro die Kosten pro Minute angegeben, z. B. 0.032 für 3,2 Cent pro Minute. Diese werden unter Berücksichtigung der Taktzeit in die tatsächlich anfallenden Kosten umgerechnet, welche dann im imon-Client oder der WebGUI angezeigt werden.
- Feld *Typ*: Dieses Feld gibt den Typ des Zeitraums an:
  - Y oder J: Im angegebenen Zeitraum wird der Circuit aktiviert, unabhängig von den anfallenden Kosten.
  - L: Im angegebenen Zeitraum wird der Circuit aktiviert, wenn er zu den günstigsten Circuits gehört. ('L' steht für 'Least cost', also "niedrigste Kosten".)
  - N: Der angegebene Zeitbereich dient nur zum Berechnen von Kosten, der Circuit wird in diesem Zeitraum jedoch nicht aktiviert. Dies kann sinnvoll sein, wenn der Circuit *manuell* aktiviert wird, etwa wenn es sich um einen Circuit zur Verbindung mit einem Firmennetz handelt, der nur bei Bedarf hinzugeschaltet wird.

Der Typ kann weggelassen werden, in diesem Fall wird 'L' angenommen.

Standard-Einstellung: `CIRC_2_TIMES='Mo-Su:00-24:0.0:N'`

Beispiel 1:

```
CIRC_1_TIMES='Mo-Fr:09-18:0.049:N Mo-Fr:18-09:0.044:L Sa-Su:00-24:0.039:Y'
```

### 3. Basiskonfiguration

Beispiel 2 für diejenigen, die eine Flatrate nutzen:

```
CIRC_2_TIMES='Mo-Su:00-24:0.0:Y'
```

**Wichtig:** Wenn die Zeitbereiche aller aktivierten Circuits mit einer Default-Route zusammengefasst nicht die komplette Woche beinhalten, gibt es zu diesen Lückenzeiten keine Default-Route. Damit ist dann das Surfen im Internet zu diesen Zeiten ausgeschlossen!

Und noch eine letzte Bemerkung: Feiertage werden wie Sonntage behandelt.

**CIRC\_x\_CHARGEINT** Mit dieser Variable wird der Zeittakt in Sekunden angegeben. Dieser wird dann für die Kosten-Berechnung verwendet.

Die meisten Provider rechnen minutengenau ab. In diesem Fall ist der Wert '60' richtig. Bei Providern mit sekundengenaue Abrechnung setzt man die Variable entsprechend auf '1'.

Diese Variable ist nur möglich bzw. sinnvoll bei Circuits, die tatsächlich Kosten verursachen. Bei Circuits, die keine Einwahl im herkömmlichen Sinne durchführen (route, dhcp), ist diese Einstellung nicht möglich.

Standard-Einstellung: CIRC\_x\_CHARGEINT='0'

Beispiel: CIRC\_x\_CHARGEINT='60'

**CIRC\_x\_HUP\_TIMEOUT** Hier kann die Zeit in Sekunden angegeben werden, nach welcher die Verbindung beendet werden soll, wenn kein Datenverkehr mehr über den Circuit läuft. Dabei steht ein Timeout von '0' für "kein Timeout", d. h. der Router legt nicht auf und wählt sich nach einem Zwangsauflegen auch sofort wieder neu ein.

Momentan wird ein Hangup-Timeout > 0 nur für ppp-Circuits unterstützt.

Diese Eigenschaft unterscheidet generell zwischen "normalen" Circuits, die sich bei der `fli4lctrl dial`-Operation sofort einwählen (Hangup-Timeout gleich null), und "dial-on-demand"-Circuits, die nach der `fli4lctrl dial`-Operation nur bereit für eine (komme)nde Einwahl sind (Hangup-Timeout größer null). Mehr Informationen hierzu finden sich in den Abschnitten "[Circuit-Zustände](#)" (Seite 94) und "[Das Programm fli4lctrl](#)" (Seite 97).

Standard-Einstellung: CIRC\_x\_HUP\_TIMEOUT='0'

Beispiel: CIRC\_x\_HUP\_TIMEOUT='600'

**CIRC\_x\_USEPEERDNS** Hiermit wird festgelegt, ob die vom Provider bei der Einwahl übergebenen DNS-Namensserver für die Dauer der Verbindung in die Konfigurationsdatei des lokalen DNS-Servers (dnsmasq) eingetragen werden sollen.

Sinnvoll ist die Nutzung dieser Option also nur bei Circuits, die entsprechende Informationen liefern. Dies betrifft i. d. R. Internet-Anbindungen via PPP und DHCP-Circuits.

Diese Option bietet den Vorteil, immer mit den am nächsten liegenden DNS-Namensservern arbeiten zu können, sofern der Provider die korrekten IP-Adressen übermittelt – dadurch geht die Namensauflösung schneller.

### 3. Basiskonfiguration

Im Falle eines Ausfalls eines DNS-Servers beim Provider werden in der Regel die übergebenen DNS-Server-Adressen sehr schnell vom Provider korrigiert.

Trotz allem ist vor jeder ersten Einwahl die Angabe eines gültigen Namensservers in `DNS_FORWARDERS` zwingend erforderlich, da sonst die erste Anfrage nicht korrekt aufgelöst werden kann. Außerdem wird beim Beenden der Verbindung die originale Konfiguration des lokalen Namensservers wieder hergestellt.

Standard-Einstellung: `CIRC_x_USEPEERDNS='no'`

Beispiel: `CIRC_x_USEPEERDNS='yes'`

**CIRC\_x\_WAIT** In der Regel wird das Wählen eines Circuits im Hintergrund durchgeführt. Will man jedoch beim Booten sicherstellen, dass sich ein Circuit erfolgreich eingewählt hat, kann man diese Variable auf die Anzahl der maximal zu wartenden Sekunden setzen. Bei '0' wird nicht gewartet.

Ein Wert größer null kann bei ppp-Circuits (d. h. wenn `CIRC_x_TYPE='ppp'` gesetzt ist) nur verwendet werden, wenn es sich um keinen Dial-on-demand-Circuit handelt, wenn also `CIRC_x_HUP_TIMEOUT='0'` gesetzt ist (bzw. die Variable gar nicht definiert wird). Der Grund hierfür ist, dass ein Warten auf einen Dial-on-demand-Circuit wenig Sinn hat, weil der Wählvorgang erst bei entsprechender Netzwerkaktivität erfolgt.

Standard-Einstellung: `CIRC_x_WAIT='0'`

Beispiel: `CIRC_x_WAIT='15'`

**CIRC\_x\_DEBUG** Mit dieser Variable können zusätzliche Debug-Ausgaben eingeschaltet werden. Dies ist Circuit-spezifisch und hat nicht zwangsläufig bei jedem Circuit-Typ sichtbare Auswirkungen.

Standard-Einstellung: `CIRC_x_DEBUG='no'`

Beispiel: `CIRC_x_DEBUG='yes'`

**CIRC\_x\_DEPS** Mit dieser Variable können Abhängigkeiten zwischen Circuits spezifiziert werden. Ein Circuit A, der von einem Circuit B abhängig ist, kann nur dann online gehen, wenn Circuit B ebenfalls online ist. Dies ist insbesondere dann nützlich, wenn Circuit A über seine Netzanbindung Infrastruktur zur Verfügung stellt, die Circuit B benötigt, etwa wenn Circuit A eine IPv4-Internetanbindung herstellt und Circuit B einen 6in4-Tunnel aufbaut.

Standard-Einstellung: `CIRC_x_DEPS=''`

Beispiel 1: `CIRC_x_DEPS='internet'`

Gelegentlich muss nicht der *gesamte* Circuit mit all seinen konfigurierten Layer-3-Protokollen online sein, damit eine Abhängigkeit erfüllt ist, sondern nur ein bestimmtes Protokoll, z.B. IPv4 oder IPv6. In diesem Fall kann man das Protokoll hinter dem Circuit angeben, mit einem Schrägstrich abgetrennt. Das folgende Beispiel zeigt eine Abhängigkeit zu einem Tag oder Circuit namens "internet", wobei es ausreicht, wenn dessen IPv4-Anbindung online ist. Dies ist z.B. für 6in4-Tunnel völlig ausreichend, denn die IPv6-Konnektivität spielt bei 6in4 naturgemäß keine Rolle (schließlich stellt ein 6in4-Tunnel gerade eine IPv6-Anbindung über eine IPv4-Anbindung her).

Beispiel 2: `CIRC_x_DEPS='internet/ipv4'`

**CIRC\_x\_CLASS\_y** Mit diesen Variablen können einem Circuit **Klassen** (Seite 97) zugeordnet werden. Durch Klassen sich Circuits logisch gruppieren, es wird somit eine Abstraktion geschaffen, die auf vielfältige Weise ausgenutzt werden kann. Eine mögliche Anwendung ist die Nutzung innerhalb von Abhängigkeiten zwischen Circuits (**CIRC\_x\_DEPS**, siehe oben), wenn mehrere Circuits eine Abhängigkeit erfüllen können.

Jede hier angegebene Klasse muss via **CIRC\_CLASS\_x\_NAME** (Seite 97) definiert werden. Ist dies nicht der Fall, wird eine Fehlermeldung ausgegeben.

Standard-Einstellung: **CIRC\_x\_CLASS\_N**='0'

Beispiel:

```
CIRC_1_NAME='DHCP-LAN'
CIRC_1_TYPE='dhcp'
CIRC_1_ENABLED='yes'
CIRC_1_DHCP_DEV='eth0'
CIRC_1_NETS_IPV4_N='1'
CIRC_1_NETS_IPV4_1='0.0.0.0/0'
CIRC_1_CLASS_N='1'
CIRC_1_CLASS_1='internet-v4'

CIRC_2_NAME='DSL-Telekom'
CIRC_2_TYPE='ppp'
CIRC_2_ENABLED='yes'
CIRC_2_PPP_TYPE='ethernet'
CIRC_2_PPP_USERID='anonymer'
CIRC_2_PPP_PASSWORD='surfer'
CIRC_2_PPP_ETHERNET_TYPE='kernel'
CIRC_2_PPP_ETHERNET_DEV='eth1'
CIRC_2_NETS_IPV4_N='1'
CIRC_2_NETS_IPV4_1='0.0.0.0/0'
CIRC_2_CLASS_N='1'
CIRC_2_CLASS_1='internet-v4'

CIRC_3_NAME='IPv6-Tunnel'
CIRC_3_TYPE='tun6in4-he'
CIRC_3_ENABLED='yes'
CIRC_3_NETS_IPV6_N='1'
CIRC_3_NETS_IPV6_1='::/0'
CIRC_3_CLASS_N='1'
CIRC_3_CLASS_1='internet-v6'
CIRC_3_DEPS='internet-v4'
```

In diesem Beispiel ist ein 6in4-HE-Tunnel (siehe Paket `ipv6`) abhängig von einem Circuit der Klasse “internet-v4”. Ob das zur Laufzeit dann die DSL- (siehe Paket `dsl`) oder DHCP-Anbindung (siehe Paket `dhcp_client`) ist, ist egal – sobald einer der beiden Circuits online ist, kann der Tunnel ebenfalls online gehen.

**CIRC\_x\_BUNDLE** Ist **CIRC\_x\_BUNDLE** nicht leer und referenziert es einen anderen gültigen Circuit, dann wird der referenzierende Circuit Teil eines so genannten “Bündels”. Gebündelte Circuits bilden zusammen *eine* logische Verbindung. Dies wird momentan nur vom Paket `ppp` unterstützt, siehe Abschnitt “**Multilink PPP**” (Seite 235).

Beispiel: CIRC\_x\_BUNDLE='internet-mp'

### 3.17.2. Circuit-Zustände

Jeder Circuit hat, während der Router läuft, einen der folgenden Zustände:

Zustand	Interner Name	Beschreibung
<i>inaktiv</i>	inactive	Ein Circuit ist <i>inaktiv</i> , wenn er nicht zur Einwahl herangezogen werden kann.
<i>aktiv</i>	active	Ein Circuit ist <i>aktiv</i> , wenn er zur Einwahl herangezogen werden kann.
<i>bereit</i>	ready	Ein Circuit ist <i>bereit</i> , wenn er sich bei Netzwerk-Aktivität automatisch einwählt (“dial-on-demand”).
<i>online</i>	online	Ein Circuit ist <i>online</i> , wenn die Verbindung erfolgreich aufgebaut werden konnte und die Netzwerk-Anbindung erfolgt ist.
<i>ausgefallen</i>	failed	Ein Circuit ist <i>ausgefallen</i> , wenn festgestellt wurde, dass die Verbindung über diesen Circuit nicht funktioniert. Dieser Zustand entspricht fast komplett dem Zustand <i>inaktiv</i> , mit dem einzigen Unterschied, dass ein ausgefallener Zustand von <code>circd</code> ignoriert wird (siehe hierzu den Abschnitt “Das Programm <code>circd</code> ” (Seite 100)). Dieser Zustand ist somit vor allem für einen automatisierten Fallback-Mechanismus gedacht.

Tabelle 3.11.: Circuit-Zustände

Die *Übergänge* zwischen diesen Zuständen werden teilweise mit `fli4lctrl` (Seite 97) durchgeführt, teilweise erfolgen sie automatisch. Ihre Bedeutung ist wie folgt:

Zustandsübergang	Beschreibung
<i>inaktiv</i> → <i>aktiv</i>	Ein Circuit wird aktiviert und kann sich je nach Wählmodus manuell oder automatisch einwählen. Zu diesem Zeitpunkt können noch keine Daten über den Circuit transportiert werden. Dieser Zustandsübergang kann in allen Wählmodi erfolgen. Er wird durch <code>fli4lctrl up</code> ausgelöst.
<i>aktiv</i> → <i>bereit</i>	Ein <i>aktiver</i> Circuit wird in den Zustand <i>bereit</i> versetzt, in dem eine Einwahl auf Grund von Netzwerk-Aktivität möglich ist. Zu diesem Zeitpunkt können noch keine Daten über den Circuit transportiert werden. In der Regel werden bei diesem Zustandsübergang Hintergrundprozesse gestartet, die für die folgenden Zustandsübergänge verantwortlich sind. Im Wählmodus <i>auto</i> erfolgt dieser Zustandsübergang direkt nach dem Übergang <i>inaktiv</i> → <i>aktiv</i> oder <i>bereit</i> → <i>aktiv</i> . Im Wählmodus <i>manual</i> muss dieser Zustandsübergang explizit durch <code>fli4lctrl dial</code> ausgelöst werden. Im Wählmodus <i>off</i> ist dieser Zustandsübergang nicht möglich.

Zustandsübergang	Beschreibung
<i>bereit</i> → <i>online</i>	Über den Circuit im Zustand <i>bereit</i> findet eine Einwahl statt. Nach deren erfolgreichem Abschluss können Daten über den Circuit transportiert werden, sofern für den Circuit entsprechende zu routende Netze (siehe <a href="#">CIRC_x_NETS_IPV4_y</a> (Seite 88) und <a href="#">CIRC_x_NETS_IPV6_y</a> (Seite 88)) konfiguriert sind. Je nach <a href="#">Hangup-Timeout</a> (Seite 91) erfolgt dieser Zustandsübergang direkt nach dem Zustandsübergang <i>aktiv</i> → <i>bereit</i> (Hangup-Timeout = 0), oder er wird durch eine Netzwerk-Aktivität ausgelöst (Hangup-Timeout > 0).
<i>online</i> → <i>bereit</i>	Die Wählverbindung wird beendet und die Netzwerk-Anbindung abgebaut. Danach können keine Daten mehr über den Circuit transportiert werden. Je nach <a href="#">Hangup-Timeout</a> (Seite 91) wird dieser Zustandsübergang entweder explizit vom Benutzer via <code>fli4lctrl hangup</code> angefordert (Hangup-Timeout = 0), oder er erfolgt automatisch nach einer gewissen Zeitspanne der Netzwerk-Inaktivität (Hangup-Timeout > 0).
<i>bereit</i> → <i>aktiv</i>	Ein Circuit im Zustand <i>bereit</i> wird wieder in den Zustand <i>aktiv</i> versetzt. Danach ist eine automatische (Wieder-)Einwahl auf Grund von Netzwerkaktivität nicht mehr möglich. In der Regel werden bei diesem Zustandsübergang Hintergrundprozesse beendet, die beim Zustandsübergang <i>aktiv</i> → <i>bereit</i> gestartet wurden. Im Wählmodus <i>manual</i> erfolgt dieser Zustandsübergang direkt nach dem Übergang <i>online</i> → <i>bereit</i> . Im Wählmodus <i>auto</i> muss dieser Zustandsübergang explizit durch <code>fli4lctrl hangup</code> ausgelöst werden. (Auf Grund der Semantik vom Wählmodus <i>auto</i> wird sofort wieder in den Zustand <i>bereit</i> gewechselt, siehe die Beschreibung von <i>aktiv</i> → <i>bereit</i> weiter oben.)
<i>aktiv</i> → <i>inaktiv</i>	Ein Circuit wird deaktiviert und kann künftig nicht mehr zur Einwahl herangezogen werden. Dieser Zustandsübergang kann in allen Wählmodi erfolgen. Er wird durch <code>fli4lctrl down</code> ausgelöst.

Tabelle 3.12.: Circuit-Zustandsübergänge

Nicht jeder Circuit unterscheidet effektiv zwischen *bereit* und *online*. So fallen diese Konzepte z.B. bei DHCP zusammen, weil es dort nicht möglich ist, einen Hangup-Timeout > 0 zu konfigurieren.

### 3.17.3. Wählmodus (DIALMODE)

Der Wählmodus steuert, ob und auf welche Art und Weise der fli4l-Router für die Einwahl verantwortlich ist. Der Wählmodus ist zum einen eine globale Eigenschaft, die das generelle Wählverhalten des fli4l kontrolliert. Es gibt drei Varianten:

Wählmodus	Beschreibung
off	In diesem Modus sind alle Circuits <i>inaktiv</i> oder <i>aktiv</i> . Der fli4l wählt weder von alleine (Netzwerkaktivität, <code>circd</code> etc.) noch auf Benutzerwunsch ( <code>fli4lctrl dial</code> , WebGUI etc.).
manual	In diesem Modus können <i>aktive</i> Circuits auf explizite Benutzeranfrage (via <code>fli4lctrl dial</code> oder über die WebGUI) in den Zustand <i>online</i> wechseln. Sowohl bei <code>fli4lctrl hangup</code> als auch bei einem konfigurierten Hangup-Timeout > 0 und entsprechend langer Netzwerk-Inaktivität wird aufgelegt, der Circuit wechselt dabei wieder in den Zustand <i>aktiv</i> . In diesem Wählmodus ignoriert <code>circd</code> die Zeitspezifikationen und schaltet keine Circuits um.
auto	In diesem Modus werden <i>aktive</i> Circuits automatisch in den Zustand <i>bereit</i> versetzt. Je nach konfiguriertem Hangup-Timeout wechselt ein solcher Circuit entweder sofort (Hangup-Timeout = 0) oder erst bei Bedarf (Hangup-Timeout > 0) in den Zustand <i>online</i> , nämlich wenn Netzwerk-Aktivität verzeichnet wird. Bei einem konfigurierten Hangup-Timeout > 0 wird bei entsprechend langer Netzwerk-Inaktivität aufgelegt, der Circuit wechselt dabei wieder in den Zustand <i>bereit</i> . Der Befehl <code>fli4lctrl dial</code> steuert hierbei <i>nicht</i> direkt die Einwahl, sondern nur, ob der Circuit <i>bereit</i> oder nicht <i>bereit</i> (d. h. nur <i>aktiv</i> ) ist. Bei externen Verbindungsabbrüchen oder beim expliziten Auflegen wird danach gleich wieder eine erneute Einwahl versucht. In diesem Wählmodus schaltet <code>circd</code> je nach Zeitspezifikation die Circuits automatisch um. <i>Ausgefallene</i> Circuits werden dabei jedoch ignoriert.

Tabelle 3.13.: Verfügbare Wählmodi

Sowohl im Wählmodus *manual* als auch im Wählmodus *auto* muss ein Circuit via `fli4lctrl up` aktiviert werden, bevor er (automatisch oder manuell via `fli4lctrl dial`) in den Zustand *bereit* wechseln kann.

Zum anderen ist der Wählmodus eine lokale Eigenschaft, die pro Circuit verwaltet wird. Der *effektive* Wählmodus ist dann das Minimum beider Wählmodi, mit der Ordnung *off* < *manual* < *auto*. Damit lässt sich z. B. erreichen, dass Circuits generell automatisch (z. B. ins Internet), einige Circuits (z. B. in die Firma) aber nur manuell gewählt werden; ein schnelles Auflegen aller Circuits ist weiterhin durch das Ändern des globalen Wählmodus auf *off* einfach zu realisieren.

Der lokale Wählmodus eines jeden Circuits ist, sofern nicht explizit via `CIRC_x_DIALMODE` (Seite 88) anders konfiguriert, initial “auto”, so dass anfangs nur der globale Wählmodus eine Rolle spielt.

**DIALMODE** Mit dieser Variable wird der initiale globale Wählmodus beim Booten festgelegt.

Eine Änderung ist im Nachhinein mit Hilfe des `fli4lctrl`-Programms, der WebGUI oder dem imon-Client möglich.

Standard-Einstellung: `DIALMODE='auto'`

Beispiel: `DIALMODE='manual'`



### 3.17.4. Circuit-Klassen

Circuit-Klassen bieten eine Möglichkeit, “artverwandte” Circuits zu gruppieren. Wenn man z. B. mehrere Möglichkeiten der Anbindung des Routers ans Internet hat, so ist doch all diesen Circuits die Default-Route gemeinsam, d. h. dass `CIRC_x_NETS_IPV4_y='0.0.0.0/0'` (für IPv4) bzw. `CIRC_x_NETS_IPV6_y='::/0'` (für IPv6) gilt. Dies kann man “herausmultiplizieren” und daraus eine eigene Klasse definieren, die man z. B. sinnigerweise “Internet” nennt:

```
CIRC_CLASS_N='1'
CIRC_CLASS_1_NAME='Internet'
CIRC_CLASS_1_NETS_IPV4_N='1'           # Circuits dieser Klasse installieren die
CIRC_CLASS_1_NETS_IPV4_1='0.0.0.0/0'   # Default-Route für IPv4...
CIRC_CLASS_1_NETS_IPV6_N='1'
CIRC_CLASS_1_NETS_IPV6_1='::/0'        # ...und für IPv6
```

Ein Circuit kann dieser Klasse “Internet” mit Hilfe der Variable `CIRC_x_CLASS_y` (Seite 93) zugeordnet werden.

Neben Routen können auch Firewall-Regeln in einer Klasse sinnvoll sein. So kann z. B. eine Port-Weiterleitung zentral für alle Internet-Circuits in der Klasse “Internet” konfiguriert werden:

```
# Fortsetzung von oben
CIRC_CLASS_1_PF_PREROUTING_N='1'
CIRC_CLASS_1_PF_PREROUTING_1='tmpl:http DNAT:@web-server'
CIRC_CLASS_1_PF_FORWARD_N='1'
CIRC_CLASS_1_PF_FORWARD_1='tmpl:http @web-server ACCEPT'
```

Diese Regeln sind dann für alle Circuits gültig, die zur Klasse “Internet” gehören.

**CIRC\_CLASS\_N** Diese Variable gibt die Anzahl der konfigurierten Circuit-Klassen an.

Standard-Einstellung: `CIRC_CLASS_N='0'`

Beispiel: `CIRC_CLASS_N='2'`

**CIRC\_CLASS\_x\_NAME** Jede Circuit-Klasse hat einen Namen. Dieser Name kann aus Buchstaben, Ziffern und dem Bindestrich ('-') bestehen. Der Name muss unter allen Circuits (siehe `CIRC_x_NAME` (Seite 87)) und Circuit-Klassen eindeutig sein.

Beispiel: `CIRC_CLASS_x_NAME='Internet'`

### 3.17.5. Das Programm `fli4lctrl`

Das Programm `fli4lctrl` ist der Zugang zum Circuit-System über die Kommandozeile. Es kann verwendet werden, um die Zustandsübergänge der Circuits herbeizuführen und um den Wählmodus zu verändern. Die möglichen Befehle lauten:

Kommando	Beschreibung
<code>up &lt;Circuit&gt;</code>	Der Circuit wird vom Zustand <i>inaktiv</i> in den Zustand <i>aktiv</i> überführt. Im Wählmodus <i>auto</i> schließt sich unmittelbar ein <code>dial &lt;Circuit&gt;</code> an, s. u.

### 3. Basiskonfiguration

Kommando	Beschreibung
<b>dial</b> <Circuit>	Der Circuit wird vom Zustand <i>aktiv</i> in den Zustand <i>bereit</i> überführt. Bei einem Hangup-Timeout = 0 folgt unmittelbar ein Wählvorgang mit dem Ziel, den Circuit in den Zustand <i>online</i> zu überführen. Bei einem Hangup-Timeout > 0 wird nicht sofort gewählt, sondern auf entsprechende Netzwerk-Aktivität gewartet. Im Wählmodus <i>off</i> wird das Kommando ignoriert.
<b>autodial</b> <Circuit>	Der Circuit wird genauso wie beim Befehl <b>fli4lctrl dial</b> vom Zustand <i>aktiv</i> in den Zustand <i>bereit</i> versetzt, aber <i>nur</i> , wenn der effektive Wählmodus des Circuits <i>auto</i> ist. In allen anderen Fällen wird der Befehl ignoriert.
<b>dial</b>	Es findet die Initiierung der Einwahl auf allen aktiven Circuits statt.
<b>hangup</b> <Circuit>	Der Circuit wird von den Zuständen <i>online</i> und <i>bereit</i> in den Zustand <i>aktiv</i> überführt. Im Wählmodus <i>auto</i> erfolgt anschließend ein <b>dial</b> <Circuit>.
<b>hangup</b>	Es findet ein Auflegen aller Circuits statt, die in den Zuständen <i>bereit</i> oder <i>online</i> sind.
<b>down</b> <Circuit>	Der Circuit wird von allen anderen Zuständen in den Zustand <i>inaktiv</i> überführt, unabhängig vom Wählmodus. Falls der Circuit vorher im Zustand <i>bereit</i> oder <i>online</i> war, wird vorher ein <b>hangup</b> <Circuit> ausgeführt, s. o.
<b>fail</b> <Circuit>	Der Circuit wird von allen anderen Zuständen in den Zustand <i>ausgefallen</i> überführt, unabhängig vom Wählmodus. Falls der Circuit vorher im Zustand <i>bereit</i> oder <i>online</i> war, wird vorher ein <b>hangup</b> <Circuit> ausgeführt, s. o.

### 3. Basiskonfiguration

Kommando	Beschreibung
<code>dialmode global</code> <Wählmodus>	<p>Der angegebene Wählmodus wird global eingestellt. Pro Circuit wird der <i>effektive</i> Wählmodus als Minimum des globalen und lokalen (s.u.) Wählmodus bestimmt. Folgende Zustandsübergänge finden statt:</p> <ul style="list-style-type: none"> <li>Ein effektiver Moduswechsel <math>* \rightarrow \text{off}</math> impliziert ein <b>hangup</b> auf allen Circuits in den Zuständen <i>bereit</i> oder <i>online</i> (dies entspricht somit einem <code>fli4lctrl hangup</code>).</li> <li>Ein effektiver Moduswechsel <math>* \rightarrow \text{manual}</math> impliziert ein <b>hangup</b> auf allen Circuits im Zustand <i>bereit</i>. Circuits im Zustand <i>online</i> legen <i>nicht</i> auf; hier greift der neue Wählmodus erst <i>nach</i> dem nächsten Auflegen.</li> <li>Ein effektiver Moduswechsel <math>* \rightarrow \text{auto}</math> impliziert ein <b>dial</b> auf allen <i>aktiven</i> Circuits (dies entspricht somit einem <code>fli4lctrl dial</code>).</li> </ul>
<code>dialmode local</code> <Circuit> <Wählmodus>	Der angegebene Wählmodus wird lokal für den Circuit eingestellt. Für die sich daraus ergebenden Zustandsänderungen siehe oben.

Tabelle 3.14.: fli4lctrl-Befehle

Kommando	Beschreibung
<code>status</code> <Circuit>	Es wird der aktuelle Zustand des zugehörigen Circuits ausgegeben.
<code>status</code>	Der aktuelle Online-Status des Routers wird ausgegeben. Der Rückgabecode ist 0, falls der Router <i>online</i> ist, und 1, falls er <i>offline</i> ist oder ein Fehler aufgetreten ist. Wann genau der Router <i>online</i> ist, wird im Abschnitt <a href="#">Wann ist mein Router online?</a> (Seite 101) erläutert.
<code>dialmode global</code>	Der aktuelle globale Wählmodus wird zurückgegeben.
<code>dialmode local</code> <Circuit>	Der aktuelle lokale Wählmodus für den angegebenen Circuit wird zurückgegeben.
<code>dialmode effective</code> <Circuit>	Der aktuelle effektive Wählmodus für den angegebenen Circuit wird zurückgegeben.
<code>list states</code>	Eine Liste aller Circuits mit den zugehörigen Zuständen wird ausgegeben.
<code>list dialmodes</code>	Eine Liste aller Circuits mit den zugehörigen lokalen und effektiven Wählmodi wird ausgegeben.

Kommando	Beschreibung
<code>list classes</code>	Eine Liste aller Circuits mit den zugehörigen Klassen wird ausgegeben.
<code>list deps</code>	Eine Liste aller Circuits mit den zugehörigen Abhängigkeiten wird ausgegeben. Erfüllte Abhängigkeiten werden entsprechend markiert.
<code>show</code>	Ein Alias für <code>list states</code> .

Tabelle 3.15.: `fli4lctrl`-Statusbefehle

Zu beachten ist, dass statt des Identifikators eines Circuits (z. B. “`circ1`”) alternativ auch

- sein Alias (z. B. “`ppp0`”),
- sein Name (z. B. “T-Com DSL”) oder
- ein aktives, ihm zugeordnetes Schlagwort (z. B. “`internet-v4`”)

verwendet werden kann.

### 3.17.6. Das Programm `circd`

Der `circd` ist ein Dämon, der anhand von Zeit-Spezifikationen Circuits automatisch im Hintergrund umschaltet. Dabei werden neben der Zeit- und Kosten-Spezifikation (`CIRC_x_TIMES`) auch die Priorität eines Circuits (`CIRC_x_PRIORITY`) sowie dessen Zustand (*ausgefallen* oder nicht) berücksichtigt.

Für einen beliebigen Zeitpunkt funktioniert das Auswählen wie folgt:

1. Zuerst werden alle Circuits gesucht, die für den betreffenden Zeitpunkt aktiviert sind (Typ ‘Y’).
2. Aus dieser Menge werden zuerst all jene betrachtet, die zur höchsten verwendeten Prioritätsklasse gehören (deren `CIRC_x_PRIORITY`-Wert also am niedrigsten ist).
3. Aus dieser Menge werden alle Circuits entfernt, die nicht nutzbar sind, die also im Zustand *ausgefallen* sind.
4. Wenn die resultierende Menge nicht leer ist, ist der Algorithmus beendet, und die resultierenden Circuits werden ausgewählt. Wenn die resultierende Menge leer ist, werden die Schritte 2 und 3 für die nächst niedrigere Prioritätsklasse wiederholt.
5. Falls alle via ‘Y’ aktivierten Circuits nicht nutzbar sind, werden alle Circuits gesucht, die für den betreffenden Zeitpunkt als LCR-Circuits vorgemerkt sind (Typ ‘L’).
6. Aus dieser Menge werden zuerst all jene betrachtet, die zur höchsten verwendeten Prioritätsklasse gehören (deren `CIRC_x_PRIORITY`-Wert also am niedrigsten ist).
7. Aus dieser Menge werden alle Circuits entfernt, die nicht nutzbar sind, die also im Zustand *ausgefallen* sind.
8. Aus dieser Menge werden diejenigen Circuits bestimmt, die am wenigsten kosten.

9. Wenn die resultierende Menge nicht leer ist, ist der Algorithmus beendet, und die resultierenden Circuits werden ausgewählt. Wenn die resultierende Menge leer ist, werden die Schritte 6 bis 8 für die nächst niedrigere Prioritätsklasse wiederholt.
10. Falls danach immer noch keine Circuits übrig bleiben, wird kein Circuit ausgewählt.

Einige Anmerkungen zum Algorithmus:

- Mit ‘Y’ aktivierte Circuits “drängeln” sich immer vor alle mit ‘L’ aktivierten Circuits. Damit ist der Nutzer in der Lage, für bestimmte Zeiträume die Least-cost-Funktionalität zu deaktivieren und die Menge der zu verwendenden Circuits explizit einzustellen. Dies ist immer dann nützlich, wenn man aus irgendwelchen Gründen auf einen bestimmten Circuit angewiesen ist, etwa weil man die Dienste des Providers in Anspruch nehmen will, auf die man nur dann Zugriff hat, wenn man sich über den Zugang des Providers einwählt.
- Bei mit ‘Y’ aktivierten Circuits werden die Kosten bei der Auswahl ignoriert, es werden somit immer *alle* Circuits derselben Prioritätsklasse *gleichzeitig* ausgewählt. Das ist konsistent mit der Bedeutung des Typs ‘Y’ (aktiviere den Circuit unabhängig von den Kosten). Will man teurere Circuits nicht mit günstigeren gleichzeitig aktivieren, muss man den teureren Circuits eine niedrigere Priorität zuordnen.
- Die Priorität wird *vor* den Kosten berücksichtigt. Damit ist der Nutzer in der Lage, auch im Least-cost-Betrieb unabhängig von den tatsächlichen Kosten Circuits zu ordnen, da die Priorität eine benutzerdefinierte und nach Belieben veränderbare Einstellung ist, die Kosten jedoch vom Provider vorgegeben sind und für eine korrekte Abrechnung keine Veränderungen zulässig sind. Circuits zuerst nach Priorität zu ordnen ist insbesondere dann vorteilhaft, wenn ein Circuit zwar günstiger ist als andere (oder gar umsonst ist), aber dafür die Datenübertragungsrate sehr langsam ist. In diesem Fall möchte man den langsamen Circuit aller Voraussicht nach nur als Fallback nutzen, also falls alle schnelleren (und teureren) Circuits ausfallen. Bei einer umgekehrten Reihenfolge (erst Kosten, dann Priorität berücksichtigen) würde immer der kostenlose und langsame Circuit ausgewählt, ohne dass man mit der Priorität irgendetwas daran verändern könnte.
- Der Algorithmus kann durchaus mehrere Circuits als Ergebnis liefern. Dies ist unproblematisch, falls die von den Circuits gerouteten Netzwerke sich nicht überlappen. Überlappenden Netzwerke führen zu einem Fehler, und es wird nur ein Circuit aktiviert (siehe hierzu die Beschreibung der Variablen `CIRC_x_UP`); eine automatische Verteilung des Datenverkehrs auf mehrere Circuits (Stichwort “Load Balancing”) ist momentan noch nicht möglich.

#### 3.17.7. Wann ist mein Router online?

Was auf den ersten Blick trivial erscheint, ist auf den zweiten Blick eine recht knifflige Frage: Wann ist ein fli4l-Router “online”? Ist nur ein Circuit definiert, ist die Frage relativ einfach zu beantworten: Der Router ist genau dann *online*, wenn der Circuit im Zustand *online* ist. Bei mehreren Circuits, die verschiedene Netze routen, sich teilweise gegenseitig ausschließen und auch u. U. keine Wählverbindung eingehen ist die Frage schon schwieriger zu beantworten. Auch einige auf der Hand liegende Ansätze liefern nicht immer die gewünschte Antwort:

### 3. Basiskonfiguration

1. *Der Router ist online, wenn mindestens ein Circuit online ist.* Diese Regelung ist ungünstig, weil bereits die Existenz einer einzigen Route den Router in den Zustand *online* versetzt, da Routen intern über Circuits abgewickelt werden. Und ein Router ohne Routen ist nicht sehr interessant. . .
2. *Der Router ist online, wenn alle Circuits online sind.* Diese Regelung ist immer dann falsch, wenn sich Circuits gegenseitig ausschließen, wenn also beispielsweise zwei DSL-Circuits konfiguriert werden, die beide eine Internet-Anbindung herstellen und deshalb nicht parallel aktiviert werden können.
3. *Der Router ist online, wenn alle Dialup-Circuits online sind.* Diese Regelung ist besser als Regelung 1, weil sie Route-Circuits ausschließt, aber auch sie löst nicht das Problem der sich ausschließenden Circuits.
4. *Der Router ist online, wenn mindestens ein Dialup-Circuit online ist.* Dies versetzt den Router in den Zustand *online*, wenn z. B. zwar eine Wählverbindung in die Firma besteht, aber die Internet-Verbindung inaktiv ist. Das kann gewünscht sein, muss aber nicht.
5. *Der Router ist online, wenn ein Circuit mit Default-Route online ist.* Diese Regelung entspricht dem Zustand vor fl4l 4.0. Dies versetzt den Router in den Zustand *offline*, wenn eine Wählverbindung in die Firma besteht, aber die Internet-Verbindung inaktiv ist. Das kann gewünscht sein, muss aber nicht.
6. *Der Router ist online, wenn für jedes konfigurierte, zu routende Netz ein Circuit online ist.* Auch diese Regelung versetzt den Router in den Zustand *offline*, wenn eine Wählverbindung in die Firma besteht, aber die Internet-Verbindung inaktiv ist. Das kann gewünscht sein, muss aber nicht.

Anstatt nun eine feste Regel vorzugeben und im Zweifelsfall genau das zu tun, was der Benutzer *nicht* erwartet, wurde ein zweistufiges Verfahren gewählt. Der Standard-Fall wählt die rückwärtskompatible Regelung 5. Alternativ kann über die Variable `CIRC_ONLINE` eine Menge von Circuits (oder Circuit-Schlagwörtern) spezifiziert werden, die für die Online-Bewertung berücksichtigt werden sollen. Sollen also sowohl Internet- als auch Firma-Anbindungen berücksichtigt werden, und werden die entsprechenden Circuits mit den Schlagwörtern “internet” und “firma” gekennzeichnet, so ist bei `CIRC_ONLINE='internet firma'` der Router *online*, wenn der “internet”- oder der “firma”-Circuit (oder beide) online sind; bei `CIRC_ONLINE='internet'` hat der Router den Zustand *offline*, wenn keine Internet-Verbindung aktiv ist, unabhängig davon, ob eine Verbindung zur Firma besteht oder nicht.

**CIRC\_ONLINE** Diese Variable beinhaltet eine Liste von Circuits (oder Schlagwörtern), die bei der Bestimmung des Online-Zustands des Routers berücksichtigt werden. Ist die Variable vorhanden und die Liste nicht leer, ist der Router genau dann *online*, wenn mindestens ein Circuit aus der Liste *online* ist bzw. wenn mindestens ein Schlagwort aus der Liste aktiv ist. Ist die Liste leer oder die Variable nicht vorhanden, greift die rückwärtskompatible Regelung, nach welcher der Router *online* ist, wenn die Default-Route aktiv ist.

Standard-Einstellung: `CIRC_ONLINE=''`

### 3.17.8. Sonstige Einstellungen

**IP\_DYN\_ADDR** Wird eine Verbindung mit dynamischer Adressvergabe verwendet, ist `IP_DYN_ADDR` auf 'yes' zu stellen, ansonsten auf 'no'. Die meisten Internet-Provider verwenden eine dynamische Adressvergabe.

Standard-Einstellung: `IP_DYN_ADDR='yes'`

**OPT\_CIRCUIT\_STATUS** Diese Variable aktiviert einen Circuit-Status-Monitor auf der dritten fli4l-Console. Diese lässt sich mit der Tastenkombination **Alt+F3** aktivieren, ein Wechseln zurück zur Login-Konsole wird mit Hilfe der Tastenkombination **Alt+F1** bewerkstelligt. Der Monitor zeigt jeden Circuit mit Namen, Typ, Alias, Schnittstelle und Status an.

Standard-Einstellung: `OPT_CIRCUIT_STATUS='no'`

Beispiel: `OPT_CIRCUIT_STATUS='yes'`

## 3.18. Spezielle Circuit-Typen im base-Paket

### 3.18.1. Circuits vom Typ "route"

Ein Circuit vom Typ "route" dient dazu, eine vorkonfigurierte *Route* zu verwalten. Das Einwählen entspricht dem Aufbau, der Route, das Auflegen dem Abbau. Ein einzelner route-Circuit kann das Routen mehrerer IPv4- und IPv6-Netze (letzteres nur bei aktivierter IPv6-Unterstützung) gleichzeitig steuern. Insofern ist ein route-Circuit flexibler als die Konfiguration einer Route via `IP_ROUTE_x`, weil dort immer nur ein Netz pro Route angegeben werden kann.

Neben den allgemeinen Circuit-Variablen, die in Abschnitt "[Circuits allgemein](#)" (Seite 86) beschrieben sind, sind zusätzlich die folgenden Angaben erforderlich:

**CIRC\_x\_ROUTE\_DEV** In dieser Variablen ist die Netzwerk-Schnittstelle vermerkt, über welche die Route geht. Diese Angabe ist optional, sofern mindestens eine Gateway-Angabe (siehe unten) vorliegt und daraus die Netzwerk-Schnittstelle abgeleitet werden kann. Es können Schnittstellen-Namen ("eth0"), Schnittstellen-Referenzen ("`IP_NET_1_DEV`", "`IPV6_NET_1_DEV`"), Circuits ("`ppp0`") und Schlagwörter ("`internet-v4`") genutzt werden, wobei Routen über dynamische, von Circuits kontrollierte Schnittstellen eher esoterischer Natur sind und nur dann verwendet werden sollten, wenn man sich über die auftretenden dynamischen Effekte im Klaren ist.

Wenn diese Variable leer ist und beide Gateway-Adressen (IPv4 und IPv6) gesetzt sind (s. u.), müssen diese derselben Schnittstelle zugeordnet sein. Das liegt daran, dass jedem Circuit genau eine Netzwerkschnittstelle zugeordnet sein muss (und nicht mehrere).

Beispiel 1: `CIRC_x_ROUTE_DEV='IP_NET_2_DEV'`

Beispiel 2: `CIRC_x_ROUTE_DEV='pppoe-v6'`

**CIRC\_x\_ROUTE\_GATEWAY\_IPV4** Diese Variable enthält die Adresse des Next-Hop-Routers (gemeinhin "Gateway" genannt) für die zu routenden IPv4-Netze. Sie kann nur dann leer sein, wenn `CIRC_x_ROUTE_DEV` gesetzt ist; in diesem Fall wird eine Route ohne Gateway generiert. Die Gateway-Adresse kann mit einem Circuit kombiniert werden, wobei Routen über dynamische, von Circuits kontrollierte Gateways eher esoterischer Natur sind und

### 3. Basiskonfiguration

nur dann verwendet werden sollten, wenn man sich über die auftretenden dynamischen Effekte im Klaren ist.

Beispiel 1: `CIRC_x_ROUTE_GATEWAY_IPV4='192.168.1.254'`

Beispiel 2 (esoterisch): `CIRC_x_ROUTE_GATEWAY_IPV4='{dhcp}0.0.0.253'`

Im letzten Beispiel wird die Gateway-Adresse dynamisch aus dem per DHCP zugewiesenen Netz (z. B. 192.168.12.0/24) und dem angegebenen Host-Anteil gebildet (in diesem Fall also 192.168.12.253). Dies ist nur dann sinnvoll, wenn man weiß, dass egal welches Netzpräfix dem fli4l-Router von dem DHCP-Server zugewiesen wird, ein bestimmter Router an der Host-Adresse 253 zu finden ist. Normalerweise sollte der via DHCP übermittelte Router alle Routen behandeln können, somit sollte man die zu routenden Netze in einem solchen Fall direkt im jeweiligen DHCP-Circuit vermerken und nicht einen route-Circuit dafür verwenden.

**CIRC\_x\_ROUTE\_GATEWAY\_IPV6** Diese Variable enthält die Adresse des Next-Hop-Routers (gemeinhin “Gateway” genannt) für die zu routenden IPv6-Netze. Es gilt all das für `CIRC_x_ROUTE_GATEWAY_IPV4` Gesagte. Weiterhin kann diese Variable nur bei aktivierter IPv6-unterstützung genutzt werden.

Beispiel 1: `CIRC_x_ROUTE_GATEWAY_IPV6='2001:db8:42::1'`

Beispiel 2 (esoterisch): `CIRC_x_ROUTE_GATEWAY_IPV6='{dhcipv6}::0:0:0:254'`



## 4. Pakete

Neben der Basisinstallation (BASE) gibt es weitere Pakete. Diese enthalten ein oder mehrere “OPTs”<sup>1</sup>, die bei Bedarf zu BASE hinzuiinstalliert werden können. Einige dieser Pakete sind Bestandteil des Basis-Paketes, andere kommen separat. Eine Übersicht über die vom fli4l-Team bereitgestellten Pakete finden Sie auf der Download-Seite (<http://www.fli4l.de/download/stabile-version/>), die von anderen Autoren bereitgestellten Pakete sind in der OPT-Datenbank ([http://extern.fli4l.de/fli4l\\_opt-db3/](http://extern.fli4l.de/fli4l_opt-db3/)) zu finden. Im folgenden werden die vom fli4l-Team bereitgestellten Pakete beschrieben.

### 4.1. Werkzeuge im Basispaket

Im Basispaket befinden sich die folgenden OPTs:

Name	Beschreibung
OPT_SYSLOGD	<a href="#">Werkzeug zum Protokollieren von Systemmeldungen</a> (Seite 105)
OPT_KLOGD	<a href="#">Werkzeug zum Protokollieren von Kernmeldungen</a> (Seite 107)
OPT_LOGIP	<a href="#">Werkzeug zum Protokollieren von WAN-IP-Adressen</a> (Seite 107)
OPT_Y2K	<a href="#">Datumskorrektur bei nicht Y2K-festen Rechnern</a> (Seite 107)
OPT_PNP	<a href="#">Installation der isapnp-Werkzeuge</a> (Seite 108)
OPT_HOTPLUG_PCI	<a href="#">Aktivierung von PCI-Hotplugging</a> (Seite 110)

#### 4.1.1. OPT\_SYSLOGD – Protokollieren von Systemmeldungen

Viele Programme verwenden die Syslog-Schnittstelle, um Meldungen auszugeben. Damit diese auch auf der Konsole sichtbar werden, muss in diesem Falle der Daemon syslogd gestartet werden.

Sind Debug-Meldungen gewünscht, stellt man OPT\_SYSLOGD auf ‘yes’, ansonsten auf ‘no’.

Siehe auch [ISDN\\_CIRC\\_x\\_DEBUG](#) (Seite 190) und [PPPOE\\_DEBUG](#) (Seite ??).

Standard-Einstellung: OPT\_SYSLOGD=‘no’

**SYSLOGD\_RECEIVER** Mit SYSLOGD\_RECEIVER kann man festlegen, ob fli4l Syslog-Nachrichten vom Netzwerk empfangen soll oder nicht.

**SYSLOGD\_DEST\_N SYSLOGD\_DEST\_x** Mit SYSLOGD\_DEST\_x gibt man Ziele an, wohin die System-Meldungen, die von syslogd entgegengenommen werden, ausgegeben werden. Im Normalfall ist dies die Konsole von fli4l, also

```
SYSLOGD_DEST_1='*.* /dev/console'
```

Möchte man eine Datei als Ziel verwenden, ist z.B. einzutragen:

---

<sup>1</sup>Abk. für “OPTionales Modul”

#### 4. Pakete

```
SYSLOGD_DEST_1='*. * /var/log/messages'
```

Ist ein sog. Loghost im Netz vorhanden, können die Meldungen auch auf diesen Rechner umgeleitet werden – unter Angabe der IP-Adresse.

Beispiel:

```
SYSLOGD_DEST_1='*. * @192.168.4.1'
```

Das @-Zeichen ist dann der IP-Adresse voranzustellen.

Wenn die Systemmeldungen an mehrere Ziele “ausgeliefert” werden sollen, ist es nötig, die Variable `SYSLOGD_DEST_N` (Anzahl der Ziele) entsprechend zu erhöhen und die Variablen `SYSLOG_DEST_1`, `SYSLOG_DEST_2` usw. zu füllen.

Der Parameter “\*. \*” bedeutet, dass sämtliche Meldungen protokolliert werden. Man kann jedoch die Meldungen für bestimmte Ziele über sog. “Prioritäten” einschränken. In diesem Fall ersetzt man das Sternchen (\*) hinter dem Punkt (.) durch eines der folgenden Schlüsselwörter:

- debug
- info
- notice
- warning (veraltet: warn)
- err (veraltet: error)
- crit
- alert
- emerg (veraltet: panic)

Die Reihenfolge in der Liste spiegelt dabei das “Gewicht” der Meldungen wider. Die Schlüsselwörter “error”, “warn” und “panic” sind veraltet und sollten nicht mehr verwendet werden.

Vor dem Punkt kann eine sog. “Facility” statt des Sternchens (\*) eingetragen werden. Eine Erklärung würde aber hier zu weit gehen. Der geneigte Leser kann hierfür eine Suchmaschine seiner Wahl bemühen. Eine Übersicht über mögliche Facilities finden sich auf den Manpages der `syslog.conf`:

<http://linux.die.net/man/5/syslog.conf>

Normalerweise ist das Sternchen aber vollkommen ausreichend. Beispiel:

```
SYSLOGD_DEST_1='*.warning @192.168.4.1'
```

Nicht nur Unix-/Linux-Rechner können als Loghost dienen, sondern auch Windows-Rechner. Auf <http://www.fli4l.de/sonstiges/links/> findet man Verweise auf entsprechende Software. Die Verwendung eines Loghosts wird dringend empfohlen, wenn eine detaillierte Protokollierung gewünscht ist. Auch hilft die Protokollierung bei der Fehlersuche. Auch imonc “versteht” als Windows-Client das Syslog-Protokoll und kann die Meldungen in einem Fenster ausgeben.

Leider lassen sich die Boot-Meldungen von fli4l nicht über `syslogd` umlenken. Jedoch kann man fli4l auch so konfigurieren, dass die Konsole ein serielles Terminal (bzw. Terminalemulation) ist. Wie das geht, steht in dem Abschnitt [Konsolen-Einstellungen](#) (Seite 35).

**SYSLOGD\_ROTATE** Mit `SYSLOGD_ROTATE` kann man festlegen, ob `fli4l` Syslog-Nachrichten einmal täglich rotiert. Es werden dabei die Meldungen der letzten `x` Tage archiviert.

**SYSLOGD\_ROTATE\_DIR** Mit der optionalen Variable `SYSLOGD_ROTATE_DIR` kann man festlegen, dass die rotierten Syslog-Dateien nicht in `/var/log/` sondern in das angegebene Verzeichnis rotiert werden.

**SYSLOGD\_ROTATE\_MAX** Mit der optionalen Variablen `SYSLOGD_ROTATE_MAX` legt man die Anzahl der archivierten/rotierten Syslog-Dateien fest.

**SYSLOGD\_ROTATE\_AT\_SHUTDOWN** Mit der optionalen Variable `SYSLOGD_ROTATE_AT_SHUTDOWN` kann man den das Rotieren beim Herunterfahren des Routers deaktivieren. Dies sollte man jedoch nur einstellen, wenn die syslog-Dateien bereits auf ein nichtflüchtiges Ziel geschrieben werden.

### 4.1.2. OPT\_KLOGD – Protokollieren von Kernelmeldungen

Viele der auftretenden Fehler – z.B. fehlgeschlagene Einwahl – werden vom Linux-Kernel direkt auf die Konsole geschrieben. Mit `OPT_KLOGD='yes'` werden diese Meldungen an den `syslogd` umgelenkt, welcher diese dann entweder in Dateien protokollieren oder an einen Loghost weiterleiten kann, s.o. Dann hat man auf der `fli4l`-Konsole (fast) Ruhe.

Empfehlung: Wenn Sie `OPT_SYSLOGD='yes'` benutzen, sollte man auch `OPT_KLOGD='yes'` setzen.  
Standard-Einstellung: `OPT_KLOGD='no'`

### 4.1.3. OPT\_LOGIP – Protokollieren von WAN-IP-Adressen

Mit `LOGIP` ist es möglich, die WAN-IP in einer Log-Datei festzuhalten. Mit Angabe von `OPT_LOGIP='yes'` wird die Funktion aktiviert.

Standard-Einstellung: `OPT_LOGIP='no'`

**LOGIP\_LOGDIR** Verzeichnis der Log-Datei festlegen

Mit `LOGIP_LOGDIR` wird das Verzeichnis festgelegt, in welchem die Log-Datei angelegt wird oder `'auto'` für autodetect.

Standard-Einstellung: `LOGIP_LOGDIR='auto'`

### 4.1.4. OPT\_Y2K – Datumskorrektur bei nicht Y2K-festen Rechnern

Meist werden `fli4l`-Router aus alten Hardware-Teilen zusammengesetzt. Dabei kann das BIOS des Mainboards nicht Y2K-fest sein. Das kann dazu führen, dass bei einer Einstellung des Datums auf den 27.05.2000 im BIOS beim nächsten Booten der 27.05.2094 im BIOS zu finden ist! Linux zeigt dann übrigens den 27.05.1994 an.

Eigentlich kann das eingestellte Datum für den `fli4l`-Router egal sein und sollte deshalb keine Rolle spielen. Wird `fli4l` jedoch als Least-Cost-Router eingesetzt, kann dies sehr wohl eine Rolle spielen.

Grund: Der 27.05.1994 war ein Freitag, der 27.05.2000 jedoch ein Samstag. Und am Wochenende gibt's günstigere Tarife bzw. günstigere Provider ...

Eine erste Lösung lautet: Das BIOS-Datum wird vom 27.05.2000 auf den 28.05.1994 gestellt. Das war ebenso ein Samstag. Damit ist das Problem aber noch nicht gänzlich gelöst, denn `fli4l`

verwendet nicht nur den Wochentag und die momentane Uhrzeit für das LC-Routing, sondern berücksichtigt auch die Feiertage.

#### **Y2K\_DAYS** – N Tage auf Systemdatum addieren

Da das gesetzte Datum genau 2191 Tage zum tatsächlichen Datum differiert, werden bei Angabe von

```
Y2K_DAYS='2191'
```

auf das BIOS-Datum 2191 Tage addiert und dieses dann als Linux-Datum gesetzt. Das BIOS-Datum bleibt davon jedoch unberührt, sonst würde beim nächsten Booten das Datum wieder das Jahr 2094 (bzw. 1994) aufweisen.

Es gibt noch eine Alternative:

Mit dem Zugriff auf einen Time-Server kann sich fli4l die aktuelle Datum/Uhrzeit aus dem Internet holen. Dafür steht das Paket [CHRONY](#) (Seite [129](#)) zur Verfügung. Beide Einstellungen lassen sich kombinieren. Das ist sinnvoll, um mit Y2K\_DAYS zunächst das Datum schon einmal zu korrigieren und anschließend über den Time-Server die genaue Uhrzeit einzustellen.

Wer mit Y2K keine Probleme hat: Variable OPT\_Y2K='no' setzen und einfach nicht mehr darüber nachdenken ...

#### **4.1.5. OPT\_PNP – Installation von isapnp tools**

Teilweise müssen ISAPnP-Karten über das Werkzeug "isapnp" konfiguriert werden. Dies betrifft insb. ISDN-Karten mit ISDN\_TYPE 7, 12, 19, 24, 27, 28, 30 und 106 – aber nur, wenn es sich auch wirklich um ISAPnP-Karten handelt.

Zur Konfiguration ist die Erstellung einer Konfigurations-Datei etc/isapnp.conf notwendig. Hier eine Kurzanleitung zur Erstellung:

- In <config>/base.txt die Variable OPT\_PNP='yes' und MOUNT\_BOOT='rw' setzen
- fli4l booten – die ISAPnP-Karte wird wahrscheinlich nicht erkannt
- Auf fli4l-Konsole eingeben:

```
pnpdump -c >/boot/isapnp.conf
umount /boot
```

Damit ist die Konfiguration auf dem Boot-Medium gespeichert.

Weiter auf PC (Unix/Linux/Windows):

- Die Datei isapnp.conf vom Boot-Medium nach <config>/etc/isapnp.conf kopieren
- isapnp.conf mit Editor öffnen, bearbeiten und abspeichern  
Die vorgegebenen Werte kann man hier beibehalten oder auch durch andere ersetzen, die man aus den möglichen Werten wählt. Relevant sind dabei die folgenden Zeilen im folgenden Beispiel:

#### 4. Pakete

```
#      Start dependent functions: priority acceptable
#      Logical device decodes 16 bit IO address lines
#      Minimum IO base address 0x0160
#      Maximum IO base address 0x0360
#      IO base alignment 8 bytes
#      Number of IO addresses required: 8
1)      (IO 0 (SIZE 8) (BASE 0x0160))
#      IRQ 3, 4, 5, 7, 10, 11, 12 or 15.
#      High true, edge sensitive interrupt (by default)
2)      (INT 0 (IRQ 10 (MODE +E
```

1) – Hier kann als „BASE“ eine Adresse zwischen die angegebene Minimum und Maximum eingegeben werden, wobei man das „base alignment“ in betracht ziehen muss. Bei mehr als einer ISA-Karte im System muss immer darauf geachtet werden, dass es hier keine Überschneidungen gibt, achte dabei auch auf die benötigte Anzahl Adressen (number of addresses required).

2) – Hier kann aus der angezeigten Liste ein IRQ eingesetzt werden. Dabei ist 2(9), 3, 4, 5 und 7 eher eine schlechte Wahl, da sich diese normalerweise mit den Seriellen und Parallelen Schnittstellen bzw der Cascadierung ins Gehege kommen.

ISA Karten können IRQs nicht teilen, deshalb darf ein für diese Karte verwendeter nicht anderweitig belegt sein.

- Die entsprechenden Daten (IRQ/IO) in die <config>/isdn.txt übernehmen
- Es ist nötig in der <config>/base.txt die OPT\_PNP Einstellung auf 'yes' zu belassen, anderenfalls werden die erforderliche Dateien nicht mit auf das Boot-Medium kopiert. Die Einstellung MOUNT\_BOOT kann man beliebig ändern.
- Neues Boot-Medium erzeugen

**Die automatisch generierte Datei ist im Unix-Format gespeichert und enthält keine CRs. Startet man unter Windows den Notepad-Editor, zeigt dieser alle Zeilen in einer einzigen Zeile an. Der DOS-Editor "edit" kann jedoch mit Unix-Dateien umgehen. Er speichert sie dann als DOS-Datei (mit CRs) ab.**

Abhilfe:

- DOS-Box starten
- In das Verzeichnis <config>/etc wechseln
- Eingeben: edit isapnp.conf
- Datei bearbeiten und abspeichern

Anschließend kann die Datei auch wieder mit Notepad bearbeitet werden.

Man kann auch unter Windows einfach den Wordpad-Editor verwenden.

Die zusätzlich generierten CRs werden beim Booten von fl4l wieder herausgefiltert. Sie stören also nicht.

Zunächst sollte man versuchen, ohne OPT\_PNP auszukommen. Wird die Karte nicht erkannt, sollte wie oben beschrieben vorgegangen werden.

Bei einem Update auf eine neuere fli4l-Version kann die früher erstellte Datei isapnp.conf weiter verwendet werden.

Standard-Einstellung: `OPT_PNP='no'`

#### 4.1.6. OPT\_HOTPLUG\_PCI – Aktivieren von PCI-Hotplugging

Mit `OPT_HOTPLUG_PCI='yes'` werden Module auf den fli4l kopiert und beim Booten geladen, die PCI-Hotplugging aktivieren, d.h. die Unterstützung für das Hinzufügen und Entfernen von PCI-Adaptern zur Laufzeit. Für diese Funktionalität muss ein passender PCI-Hotplug-Controller vorhanden sein.

Für das Hinzufügen und Entfernen von virtuellen Geräten in *Virtualisierungsumgebungen* wie KVM muss diese Option *nicht* aktiviert sein, da dies über ACPI-Mechanismen geschieht und der zugehörige ACPI-Treiber dauerhaft im Kernel aktiviert ist.

## 4.2. Kernel 5.4

Dieses Kapitel dokumentiert die verfügbaren Treiber des Linux-Kernels in der Version 5.4, bereitgestellt vom Paket `kernel_5_4`.

### 4.2.1. Netzwerkkartentreiber

Dieser Abschnitt listet alle von diesem Kernel unterstützten Netzwerkkartentreiber auf. Dabei wird zwischen LAN-Treibern für kabelgebundene Netzwerke und WLAN-Treibern für drahtlose Netzwerke unterschieden. Treiber für drahtlose Netzwerke benötigen zusätzlich zum base- und diesem Kernel-Paket das Paket “wlan”.

Tabelle 4.1.: Verfügbare LAN-Adapter-Treiber in Linux 5.4

Bus	NET_DRV_x	Kartenfamilie
pcmcia	3c574_cs	3Com 3c574 series PCMCIA ethernet
pcmcia	3c589_cs	3Com 3c589 series PCMCIA ethernet
usb	asix	ASIX AX8817X based USB 2.0 Ethernet Devices
usb	atusb	ATUSB IEEE 802.15.4
usb	ax88179_178a	ASIX AX88179/178A based USB 3.0/2.0 Gigabit Ethernet Devices
pcmcia	axnet_cs	Asix AX88190 PCMCIA ethernet
usb	catc	CATC EL1210A NetMate USB Ethernet
usb	cdc_eem	USB CDC EEM
usb	cdc_ether	USB CDC Ethernet devices
usb	cdc_mbim	USB CDC MBIM host
usb	cdc_ncm	USB CDC NCM host
usb	cdc_subset	Simple 'CDC Subset' USB networking links
usb	ch9200	QinHeng CH9200 USB Network device
usb	cx82310_eth	Conexant CX82310-based ADSL router USB ethernet
usb	dm9601	Davicom DM96xx USB 10/100 ethernet devices

(wird auf der nächsten Seite fortgesetzt)

#### 4. Pakete

Tabelle 4.1.: Verfügbare LAN-Adapter-Treiber in Linux 5.4 (fortgesetzt)

Bus	NET_DRV_x	Kartenfamilie
virtual	dummy	Dummy Network Interface
pcmcia	fmvj18x_cs	fmvj18x and compatible PCMCIA ethernet
usb	gl620a	GL620-USB-A Host-to-Host Link cables
usb	hso	USB High Speed Option
usb	huawei_cdc_ncm	USB CDC NCM host driver with encapsulated protocol support
usb	int51x1	Intellon usb powerline adapter
usb	ipheth	Apple iPhone USB Ethernet
usb	kalmia	Samsung Kalmia USB network
usb	kaweth	KL5USB101 USB Ethernet
usb	lan78xx	LAN78XX USB 3.0 Gigabit Ethernet Devices
usb	lg-vl600	LG-VL600 modem's ethernet link
usb	mcs7830	USB to network adapter MCS7830)
usb	net1080	NetChip 1080 based USB Host-to-Host Links
pcmcia	nmclan_cs	New Media PCMCIA ethernet
pcmcia	pcnet_cs	NE2000 compatible PCMCIA ethernet
usb	pegasus	Pegasus/Pegasus II USB Ethernet
usb	plusb	Prolific PL-2301/2302/25A1/27A1 USB Host to Host Link
usb	qmi_wwan	Qualcomm MSM Interface (QMI) WWAN
usb	r8152	Realtek RTL8152/RTL8153 Based USB Ethernet Adapters
usb	rndis_host	USB Host side RNDIS
usb	rtl8150	rtl8150 based usb-ethernet
pcmcia	smc91c92_cs	SMC 91c92 series PCMCIA ethernet
usb	smc75xx	SMSC75XX USB 2.0 Gigabit Ethernet Devices
usb	smc95xx	SMSC95XX USB 2.0 Ethernet Devices
usb	sr9700	SR9700 one chip USB 1.1 USB to Ethernet device from <a href="http://www.corechip-sz.com/">http://www.corechip-sz.com/</a>
usb	sr9800	SR9800 USB 2.0 USB2NET Dev : <a href="http://www.corechip-sz.com">http://www.corechip-sz.com</a>
pcmcia	xirc2ps_cs	Xircom PCMCIA ethernet
usb	zaurus	Sharp Zaurus PDA, and compatible products

Tabelle 4.2.: Verfügbare WLAN-Adapter-Treiber in Linux 5.4

Bus	NET_DRV_x	Kartenfamilie
usb	8192cu	Realtek Wireless Lan
isa	airo	Cisco/Aironet 802.11 wireless ethernet cards

*(wird auf der nächsten Seite fortgesetzt)*

Tabelle 4.2.: Verfügbare WLAN-Adapter-Treiber in Linux 5.4 (fortgesetzt)

Bus	NET_DRV_x	Kartenfamilie
pcmcia	airo_cs	Cisco/Aironet 802.11 wireless ethernet cards
usb	ar5523	Atheros AR5523 based USB dongles
usb	at76c50x-usb	Atmel at76x USB Wireless LAN
usb	ath6kl_usb	Driver support for Atheros AR600x USB devices
usb	ath9k_htc	Atheros driver 802.11n HTC based wireless devices
pcmcia	atmel_cs	Atmel at76c50x 802.11 wireless ethernet cards
pci	b43	Broadcom B43 wireless
pci	b43legacy	Broadcom B43legacy wireless
usb	brcmfmac	Broadcom 802.11 wireless LAN fullmac
pci	brcmsmac	Broadcom 802.11n wireless LAN
usb	carl9170	Atheros AR9170 802.11n USB wireless
pcmcia	hostap_cs	Intersil Prism2-based 802.11 wireless LAN cards (PC Card)
pcmcia	libertas_cs	Marvell 83xx compact flash WLAN cards
usb	libertas_tf_usb	8388 USB WLAN Thinfirm
virtual	mac80211_hwsim	Software simulator of 802.11 radio(s) for mac80211
usb	mt7601u	
usb	mwifiex_usb	Marvell WiFi-Ex USB Driver version1.0
pcmcia	orinoco_cs	PCMCIA Lucent Orinoco, Prism II based and similar wireless cards
usb	orinoco_usb	Orinoco wireless LAN cards using EZUSB bridge
usb	p54usb	Prism54 USB wireless
pcmcia	ray_cs	Raylink/WebGear wireless LAN
usb	rndis_wlan	RNDIS based USB Wireless adapters
usb	rsi_usb	Common USB layer for RSI drivers
usb	rt2500usb	Ralink RT2500 USB Wireless LAN
usb	rt2800usb	Ralink RT2800 USB Wireless LAN
usb	rt73usb	Ralink RT73 USB Wireless LAN
usb	rtl8187	RTL8187/RTL8187B USB wireless
usb	rtl8192cu	Realtek 8192C/8188C 802.11n USB wireless
usb	rtl8xxxu	RTL8XXXu USB mac80211 Wireless LAN
usb	sierra_net	USB-to-WWAN Driver for Sierra Wireless modems
pcmcia	spectrum_cs	Symbol Spectrum24 Trilogy cards with firmware downloader
usb	usb8xxx	8388 USB WLAN
pcmcia	wl3501_cs	Planet wl3501 wireless
usb	zd1201	ZyDAS ZD1201 based USB Wireless adapters
usb	zd1211rw	USB driver for devices with the ZD1211 chip



### 4.3. Advanced Networking

Das Advanced Networking Paket beinhaltet die Möglichkeit den fli4l-Router um VLAN, Bonding und Bridging Funktionen zu erweitern. Zusätzlich gibt es die Möglichkeit EBTables (<http://ebtables.sourceforge.net/>) Unterstützung zu aktivieren. Damit wird es möglich einen transparenten Paketfilter aufzubauen.

Generell gilt bei allen Paketen aus dem advanced\_networking Paket:

**Dieses Paket ist nur für Anwender gedacht, die sich sehr gut im Bereich Netzwerke auskennen. Insbesondere sind fundierte Routingkenntnisse notwendig.**

Gerade beim aktivieren der EBTables Unterstützung können sehr ungewöhnliche Probleme auftreten, wenn man sich nicht 100% mit den verschiedenen Wirkungsweisen von Layer 2 und 3 auskennt. Einige Paketfilterregeln arbeiten mit aktivierter EBTables Unterstützung vollkommen anders als gewohnt.

#### 4.3.1. Broadcast Relay - Weiterleitung von IP Broadcasts

Mithilfe eines Broadcast Relays können IP Broadcasts über Interface-Grenzen hinweg weitergeleitet werden. Dies ist notwendig für Applikationen, die Geräte im Netzwerk mittels Broadcast ermitteln (z.B. QNAP Finder), da Broadcasts normalerweise von Routern nicht über Netzgrenzen hinweg weitergegeben werden. Durch Einrichtung eines Broadcast Relays kann dieses Problem umgangen werden.

Innerhalb eines Broadcast Relays werden Broadcasts immer an alle angeschlossenen Interfaces weitergeleitet. Das bedeutet, dass eine Einrichtung eines weiteren Broadcast Relays mit vertauschten Interfaces nicht notwendig ist. Außerdem sind mehrere Broadcast Relays, die das gleiche Interface beinhalten, nicht erlaubt.

**OPT\_BCRELAY** Weiterleiten von Broadcasts

Default: OPT\_BCRELAY='no'

Mit 'yes' wird das Broadcast Relay Paket aktiviert. Die Einstellung 'no' deaktiviert das Broadcast Relay Paket komplett.

**BCRELAY\_N** Default: BCRELAY\_N='0'

Die Anzahl der zu konfigurierenden Broadcast Relays.

**BCRELAY\_x\_IF\_N** Default: BCRELAY\_x\_IF\_N='1'

Anzahl der Interfaces, die diesem Broadcast Relay zugeordnet sind.

**BCRELAY\_x\_IF\_x** Default: BCRELAY\_x\_IF\_x=""

Name des Interfaces, das diesem Broadcast Relay zugeordnet werden soll.

Zur Verdeutlichung folgt ein Beispiel, bei dem der Rechner mit der Applikation (z.B. QNAP Finder) im internen Netzwerk (angeschlossen an eth0) hängt und das NAS sich in einem anderen Netzwerk (angeschlossen an eth1) befindet.

```
OPT_BCRELAY='yes'
BCRELAY_N='1'
BCRELAY_1_IF_N='2'
BCRELAY_1_IF_1='eth0'
BCRELAY_1_IF_2='eth1'
```

### 4.3.2. Bonding - mehrere Netzwerkkarten zusammenfassen zu einem Link

Unter Bonding versteht man das Zusammenfassen von mindestens zwei Netzwerkkarten, die auch unterschiedlichen Typs (also 3Com und Intel) und Geschwindigkeit (10 Mbit/s oder 100 Mbit/s) sein können, zu einer gemeinsamen Verbindung. Dabei können entweder entsprechende Linux Rechner direkt verbunden werden, oder eine Verbindung zu einem Switch aufgebaut werden. So kann z.B. ohne grossen Aufwand eine 200 Mbit/s Full-Duplex Verbindung vom fli4l-Router zu einem Switch geschaltet werden. Jeder der sich für Bonding interessiert sollte vorher die Dokumentation dazu im Kernelverzeichnis (bonding.txt) gelesen haben. Die Namen der Bondingeinstellungen entsprechen weitestgehend den dort verwendeten Namen. Unter dem Linuxkernel 2.6.x findet sich im Verzeichnis der Kernelsourcen unter Documentation/networking die Datei bonding.txt.

**OPT\_BONDING\_DEV** Default: OPT\_BONDING\_DEV='no'

Mit 'yes' wird das Bonding Paket aktiviert. Die Einstellung 'no' deaktiviert das Bonding Paket komplett.

**BONDING\_DEV\_N** Default: BONDING\_DEV\_N='0'

Die Anzahl der zu konfigurierenden Bondinggeräte.

**BONDING\_DEV\_x\_DEVNAME** Default: BONDING\_DEV\_x\_DEVNAME=""

Der Name des Bondinggerätes das erstellt werden soll. Der Name muß dabei mit 'bond' beginnen und es muß eine Zahl ohne führende '0' folgen. Die Namen der Bondinggeräte müssen nicht mit '0' beginnen und müssen nicht aufeinanderfolgend sein. Mögliche Werte wären z.B. 'bond0', 'bond8' oder 'bond99'.

**BONDING\_DEV\_x\_MODE** Default: BONDING\_DEV\_x\_MODE=""

Gibt eines der Bonding-Methoden an. Der Standardwert ist Round-Robin 'balance-rr'. Mögliche Werte sind hier aufgelistet:

**balance-rr** Round-Robin-Methode: Übermittle der Reihe nach über alle Slaves von ersten bis zum letzten. Diese Methode bietet sowohl Load- Balancing als auch Fehlertoleranz.

**active-backup** Aktives Backup: Nur ein Slave im Bond ist aktiv. Die anderen Slaves werden nur dann aktiviert, wenn der aktive Slave ausfällt. Die MAC-Adresse des Bonds ist nur auf einem Port (Netzwerkadapter) sichtbar, um den Switch nicht zu verwirren. Dieser Modus bietet Fehlertoleranz.

**balance-xor** XOR-Methode: Übermittle basierend auf der Formel [ (Quell-MAC-Adresse XOR Ziel-MAC-Adresse) modulo Anzahl der Slaves ]. Dadurch wird immer der selbe Slave für die selben Ziel-MAC-Adresse benutzt. Diese Methode bietet sowohl Load-Balancing als auch Fehlertoleranz.

**broadcast** Broadcast-Methode: Übermittelt alles auf allen Slave-Devices. Dieser Modus bietet Fehlertoleranz.

**802.3ad** Dynamische IEEE 802.3ad Verbindungsaggregation. Erstellt Aggregationsgruppen, die die selben Geschwindigkeits und Duplex- Einstellungen teilen. Übermittelt auf allen Slaves im aktiven Aggregator.

Voraussetzungen:

- Unterstützt für ethtool im Basistreiber, um Geschwindigkeit und Duplex-Status für jede Device abzufragen.
- Ein Switch, der dynamische IEEE 802.3ad Verbindungsaggregation unterstützt.

**balance-tlb** Adaptive Load-Balancing für ausgehende Daten: Kanal-Bonding, dass keine speziellen Features im Switch benötigt. Der ausgehende Netzwerktraffic wird entsprechend der momentanen Last (relativ zur Geschwindigkeit berechnet) auf jeden Slave verteilt. Eingehender Netzwerktraffic wird vom aktuellen Slave empfangen. Wenn der empfangende Slave ausfällt, übernimmt ein anderer Slave die MAC-Adresse des ausgefallenen Empfangsslaves.

Voraussetzungen:

Unterstützt für ethtool im Basistreiber, um Geschwindigkeit und Duplex-Status für jede Device abzufragen.

**balance-alb** Adaptive Load-Balancing: schliesst sowohl balance-tlb, als auch Eingehendes Load-Balancing (rlb) für IPv4 Traffic ein und benötigt keine speziellen Voraussetzungen beim Switch. Load-Balancing für eingehenden Traffic wird über ARP-Absprache erreicht. Der Bonding-Treiber fängt ARP-Antworten vom Server auf ihrem Weg nach aussen hin ab und überschreibt die Quell-Hardware-Adresse mit der eindeutigen HW-Adresse eines Slaves im Bond, so dass unterschiedliche Clients unterschiedliche HW-Adressen für den Server verwenden.

Eingehender Traffic von Verbindungen, die vom Server erstellt wurden wird auch verteilt. Wenn der Server ARP-Anfragen sendet, kopiert und speichert der Bonding-Treiber die Client-IP aus dem ARP. Wenn die ARP-Antwort des Client ankommt, wird seine HW-Adresse ermittelt und der Bonding-Treiber erstellt eine ARP-Antwort an diesen Client und ordnet ihn so zu einem Client im Bond zu. Ein Problematischer Effekt von ARP-Absprachen für die Lastverteilung ist, dass jedes Mal wenn eine ARP-Anfrage übermittelt wird, sie die HW-Adresse des Bonds benutzt. Also lernen die Clients die HW-Adresse des Bonds und der eingehende Traffic auf dem aktuellen Slave bricht zusammen. Diesem Umstand wird begegnet, indem Updates (ARP-Antworten) zu allen Clients mit ihrer jeweiligen HW-Adresse gesandt wird, sodass der Traffic wieder aufgeteilt ist. Eingehender Traffic wird auch dann neu aufgeteilt, wenn ein neuer Slave zum Bond hinzugefügt wird oder ein inaktiver Slave reaktiviert wird. Die Empfangslast wird der Reihe nach (Round-Robin) in der Gruppe der Slave mit der grössten Geschwindigkeit im Bond verteilt.

Wenn eine Verbindung wiederhergestellt wird oder ein neuer Slave zum Bond hinzukommt wird der eingehende Traffic neu auf alle aktiven Slaves im Bond verteilt, indem ARP-Antworten mit den ausgewählten MAC-Adressen zu jedem Client gesandt werden. Der Parameter updelay muss auf einen Wert grösser oder gleich der Weiterleitungsverzögerung (forwarding delay) des Switchs eingestellt sein, sodass ARP-Antworten an die Clients nicht vom Switch geblockt werden.

Voraussetzungen:

- Unterstützt für ethtool im Basistreiber, um Geschwindigkeit und Duplex-Status für jede Device abzufragen.
- Unterstützung im Basistreiber, die HW-Adresse auch dann setzen zu können, wenn das Device offen ist. Das ist notwendig, damit immer ein Slave im Team die

HW-Adresse des Bonds tragen kann, (der `curr_active_slave`) obwohl jeder Slave im Bond eine eigene, eindeutige HW-Adresse hat. Wenn der `curr_active_slave` ausfällt, wird seine HW-Adresse mit dem neuen `curr_active_slave` ausgetauscht.

**BONDING\_DEV\_x\_DEV\_N** Default: `BONDING_DEV_x_DEV_N='0'`

Gibt an, aus wievielen Geräten dieses Bondinggeräte besteht. Wenn z.B. ein Bondinggerät aus 'eth0' und 'eth1' gebildet werden soll muß hier eine '2' (für die beiden eth-Geräte) eingetragen werden.

**BONDING\_DEV\_x\_DEV\_x** Default: `BONDING_DEV_x_DEV_x=""`

Der Name eines Gerätes, welches zu diesem Bondinggerät gehören soll. Ein möglicher Wert wäre z.B. 'eth0'. Bitte beachten Sie, dass ein Gerät, welches Sie für ein Bondinggerät benutzen, exklusiv dafür benutzt werden muß. Insbesondere ist es nicht möglich das Gerät für ein DSL-Modem, eine Bridge, ein VLAN oder in der base.txt zu benutzen.

**BONDING\_DEV\_x\_MAC** Default: `BONDING_DEV_x_MAC=""`

Diese Einstellung ist optional und kann auch komplett weggelassen werden.

Ein Bondinggerät benutzt standardmäßig die MAC Adresse des ersten Gerätes, welches für das Bonding benutzt wird. Wenn Sie dies nicht wollen können Sie auch eine MAC Adresse angeben, die das Bondinggerät benutzen soll.

**BONDING\_DEV\_x\_MIIMON** Default: `BONDING_DEV_x_MIIMON='100'`

Diese Einstellung ist optional und kann auch komplett weggelassen werden.

Gibt an in welchen Zeitabständen (in Millisekunden) die einzelnen Verbindungen eines Bondinggerätes auf Ihren Linkstatus geprüft werden. Es wird also der Linkstatus jedes einzelnen Gerätes dieses Bondinggerätes alle x Millisekunden geprüft. Mit '0' wird die MIIMON Überwachung deaktiviert.

**BONDING\_DEV\_x\_USE\_CARRIER** Default: `BONDING_DEV_x_USE_CARRIER='yes'`

Diese Einstellung ist optional und kann auch komplett weggelassen werden.

Wenn eine Überwachung des Linkstatus per MIIMON aktiviert wird kann man hier auswählen, ob die Überwachung des Linkstatus durch die `netif_carrier_ok()` Funktion (bei der Einstellung 'yes') erfolgen soll, oder durch direkte Aufrufe von `MII` oder `ETHTOOL` `ioctl()` Systemaufrufen (mit der Einstellung 'no'). Die `netif_carrier_ok()` Methode ist effizienter, aber nicht alle Treiber unterstützen diese Methode.

**BONDING\_DEV\_x\_UPDELAY** Default: `BONDING_DEV_x_UPDELAY='0'`

Diese Einstellung ist optional und kann auch komplett weggelassen werden.

Der Wert dieser Einstellung multipliziert mit der Einstellung von `BONDING_DEV_x_MIIMON` gibt an nach welcher Zeit eine Verbindung des Bondinggerätes aktiviert wird wenn der entsprechende Link (z.B. ein eth-Gerät) aufgebaut wurde. Damit wird eine Verbindung des Bondinggerätes solange aktiviert, bis der Linkstatus auf 'nicht verbunden' schaltet.

**BONDING\_DEV\_x\_DOWNDELAY** Default: `BONDING_DEV_x_DOWNDELAY='0'`

Diese Einstellung ist optional und kann auch komplett weggelassen werden.

Der Wert dieser Einstellung multipliziert mit der Einstellung von `BONDING_DEV_x_MIIMON` gibt an nach welcher Zeit eine Verbindung des Bondinggerätes deaktiviert wird wenn der entsprechende Link (z.B. ein eth-Gerät) ausfällt. Damit wird also eine Verbindung des Bondinggerätes zeitweise deaktiviert, solange bis der Linkstatus wieder auf 'aktiv' schaltet.

**BONDING\_DEV\_x\_LACP\_RATE** Default: `BONDING_DEV_x_LACP_RATE='slow'`

Diese Einstellung ist optional und kann auch komplett weggelassen werden.

Wenn bei `BONDING_DEV_x_MODE=""` der Wert '802.3ad' eingestellt wird, kann man hier angeben wie oft die Linkinformationen mit dem Verbindungspartner (also einem Switch oder einem anderen Linuxrechner) ausgetauscht werden. 'slow' tauscht alle 30 Sekunden die Linkinformationen aus, bei 'fast' werden die Linkinformationen jede Sekunde ausgetauscht.

**BONDING\_DEV\_x\_PRIMARY** Default: `BONDING_DEV_x_PRIMARY=""`

Diese Einstellung ist optional und kann auch komplett weggelassen werden.

Wenn als Mode 'active-backup' eingestellt bestimmt man hiermit, welches Gerät primär als Ausgabegerät benutzt werden soll. Das ist vor allem sinnvoll, wenn die unterschiedlichen Geräte eine unterschiedliche Geschwindigkeit haben. Ein String (eth0, eth2, etc) der als Primäres Devices verwendet werden soll. Wenn ein Wert eingegeben wird, und das Device ist online, wird es als erstes Ausgabemedium benutzt. Nur wenn das Device offline ist, wird ein anderes Devices benutzt. Andernfalls, sobald ein Ausfall erkannt wird, wird ein neues Standardausgabemedium bestimmt. Dies ist dann praktisch, wenn ein Slave Vorrang gegenüber einem anderen haben soll - wenn bspw. ein Slave 1000 Mbit/s schnell ist und ein anderer 100 Mbit/s. Wenn der 1000 Mbit/s-Slave ausfällt und später wieder hergestellt wurde, kann es von Vorteil sein, dass der schnellere Slave wieder aktiv gesetzt werden kann, ohne beim 100 Mbit/s-Slave künstlich einen Ausfall herbeizuführen.

**BONDING\_DEV\_x\_ARP\_INTERVAL** Default: `BONDING_DEV_x_ARP_INTERVAL='0'`

Diese Einstellung ist optional und kann auch komplett weggelassen werden.

Gibt die Frequenz in Millisekunden an nach dem die unter `BONDING_DEV_x_ARP_IP_TARGET_x` angegebenen IP-Adressen (bzw. deren ARP Antwort) geprüft werden. Wenn ARP-Überwachung im Load-Balancing-Mode (mode 0 or 2) genutzt werden soll, sollte der Switch so eingestellt werden, dass er alle Pakete gleich auf alle Verbindungen verteilt - wie etwa Round-Robin. Wenn der Switch so eingestellt ist, dass er die Pakete nach der XOR-Methode verteilt, werden alle Antworten der ARP-Ziele auf der selben Verbindung ankommen und das könnte bei den anderen Team-Mitgliedern zum Ausfall führen. ARP-Überwachung sollte nicht zusammen mit miimon verwandt werden. Wird als Wert 0 übergeben, ist ARP-Überwachung deaktiviert.

**BONDING\_DEV\_x\_ARP\_IP\_TARGET\_N** Default: `BONDING_DEV_x_ARP_IP_TARGET_N=""`

Diese Einstellung ist optional und kann auch komplett weggelassen werden.

Die Anzahl der IP-Adressen die für die ARP Prüfung benutzt werden sollen. Es können maximal 16 IP-Adressen überprüft werden.

**BONDING\_DEV\_x\_ARP\_IP\_TARGET\_x** Default: `BONDING_DEV_x_ARP_IP_TARGET_x=""`

Diese Einstellung ist optional und kann auch komplett weggelassen werden.

Hier wird jeweils eine IP-Adressen angegeben, wenn `BONDING_DEV_x_ARP_INTERVAL > 0` ist. Diese werden als Ziele der ARP-Anfragen verwandt, die verschickt werden, um die Qualität der Verbindung zu den Zielen festzustellen. Geben sie diese Werte im Format `ddd.ddd.ddd.ddd` an. Damit ARP-Überwachung funktioniert, muss zumindest eine IP-Adresse angegeben werden.

### 4.3.3. VLAN - 802.1Q Unterstützung

Die Unterstützung für VLAN nach 802.1Q ist nur in Verbindung mit entsprechenden Switches sinnvoll. Port-Based VLAN Switches sind *nicht* dafür geeignet. Eine allgemeine Einführung in das Thema VLAN findet sich unter [http://www.hoteltravelmovie.de/chrisi/downloads/VLAN\\_802frame.pdf](http://www.hoteltravelmovie.de/chrisi/downloads/VLAN_802frame.pdf) in deutscher Sprache. Gerade für den Einstieg in das Thema VLAN ist diese Seite geeignet. Auf der Seite <http://de.wikipedia.org/wiki/VLAN> finden sich auch noch ein wenig Informationen wo man etwas nachlesen kann.

Bitte beachten Sie, dass nicht jede Netzwerkkarte mit VLANs umgehen kann. Einige Netzwerkkarten können überhaupt nicht mit VLANs umgehen, andere benötigen eine angepasste MTU und einige wenige Karten arbeiten vollkommen problemlos. Der Autor des `advanced_networking` Paketes benutzt Intelnetzwerkkarten mit dem 'e100' Treiber ohne jedes Problem, eine MTU Anpassung ist nicht notwendig. Der 3COM '3c59x' Treiber benötigt eine MTU Anpassung, die MTU muß auf 1496 eingestellt werden, sonst arbeitet die Karte nicht korrekt. Der 'starfire' Treiber arbeitet nicht korrekt wenn ein VLAN Gerät in einer Bridge aufgenommen wird. In diesem Fall können keine Pakete mehr empfangen werden. Wer also mit VLANs arbeiten will sollte sicherstellen, dass der jeweilige Linux Netzwerkkartentreiber VLANs auch korrekt unterstützt.

**OPT\_VLAN\_DEV** Default: `OPT_VLAN_DEV='no'`

Mit 'yes' wird das VLAN Paket aktiviert, mit 'no' wird es deaktiviert.

**VLAN\_DEV\_N** Default: `VLAN_DEV_N=""`

Anzahl der zu konfigurierenden VLAN Geräte.

**VLAN\_DEV\_x\_DEV** Default: `VLAN_DEV_x_DEV=""`

Der Name des Gerätes, das an den VLAN fähigen Switch angeschlossen ist. Das kann z.B. 'eth0', 'br1' oder 'eth2' sein.

**VLAN\_DEV\_x\_VID** Default: `VLAN_DEV_x_VID=""`

Die VLAN ID, für welches das entsprechende VLAN Gerät erstellt werden soll. Der Name des VLAN Gerätes wird aus dem Prefix 'ethX' und der angehängten VLAN ID (ohne führende '0') erstellt. Wird hier z.B. '42' eingetragen existiert später auf dem fli4l-Router das VLAN Gerät 'eth0.42'.

Die VLAN Geräte auf dem fli4l-Router heissen immer '<device>.<vid>'. Also wenn ich ein eth-Gerät habe was an einem VLAN-fähigen Switch angeschlossen ist und ich auf dem fli4l-Router die VLANs 10, 11 und 23 nutzen will konfiguriere ich 3 VLAN Geräte mit dem eth-Gerät als `VLAN_DEV_x_DEV='ethX'` und der jeweiligen VLAN ID unter `VLAN_DEV_x_VID=""`. Aber wie immer sagt ein Beispiel mehr als tausend Worte, daher hier das passende Beispiel:

```
OPT_VLAN_DEV='yes'
VLAN_DEV_N='3'
VLAN_DEV_1_DEV='eth0'
VLAN_DEV_1_VID='10' # Ergibt device: eth0.10
VLAN_DEV_2_DEV='eth0'
VLAN_DEV_2_VID='11' # Ergibt device: eth0.11
VLAN_DEV_3_DEV='eth0'
VLAN_DEV_3_VID='23' # Ergibt device: eth0.23
```

Bitte immer daran denken die MTU aller beteiligten Geräte zu prüfen. Durch den VLAN Header werden die Frame 4 Bytes länger. Wenn es notwendig ist muss bei den entsprechenden Geräten die MTU auf 1496 geändert werden.

#### 4.3.4. Device MTU - Anpassen der MTU

Unter seltenen Umständen kann es notwendig sein, die MTU eines Gerätes anzupassen. Z.B. einige nicht 100% VLAN kompatible Netzwerkkarten benötigen eine Anpassung der MTU. Bitte denken Sie daran, dass nur wenige Netzwerkkarten in der Lage sind Ethernetframes die größer als 1500 Bytes sind zu verarbeiten!

**DEV\_MTU\_N** Default: DEV\_MTU\_N="

Diese Einstellung ist optional und kann auch komplett weggelassen werden.

Gibt die Anzahl der Geräte an deren MTU geändert werden soll.

**DEV\_MTU\_x** Default: DEV\_MTU\_x="

Diese Einstellung ist optional und kann auch komplett weggelassen werden.

Der Gerätenamen dessen MTU geändert werden soll gefolgt von der einzustellenden MTU. Beide Angaben werden durch ein Leerzeichen getrennt. Um z.B. für 'eth0' eine MTU von '1496' einzustellen geben Sie folgendes ein:

```
DEV_MTU_N='1'
DEV_MTU_1='eth0 1496'
```

#### 4.3.5. BRIDGE - Ethernet Bridging für fli4l

Hierbei handelt sich um eine vollwertige Ethernet-Bridge, die bei Bedarf nach dem Spanning Tree Protokoll arbeiten kann. Für den Anwender scheint der Rechner an den konfigurierten Ports danach wie ein Layer 3 Switch zu arbeiten.

Weiterführende Informationen zum Thema Bridging finden Sie hier:

Die Homepage des Linux Bridge Projektes: <http://bridge.sourceforge.net/>.

Die ausführliche und verbindliche Beschreibung des Bridging Standards: <http://standards.ieee.org/getieee802/download/802.1D-2004.pdf>. Vor allem die Informationen ab Seite 153 sind interessant. Bitte beachten Sie, dass der Linux Bridging Code noch nach dem Standard von 1998 arbeitet. Dort gibt es z.B. nur 16 Bit Werte für die Pathcost.

Hier kann man sich die unterschiedlichen Zeitwerte für das Spanning Tree Protokoll berechnen lassen: <http://www.dista.de/netstpclc.htm>

#### 4. Pakete

Wie STP arbeitet kann man auf dieser Seite anhand einiger netter Beispiele sehen: <http://web.archive.org/web/20060114052801/http://www.zyxel.com/support/supportnote/ves1012/app/stp.htm>

**OPT\_BRIDGE\_DEV** Default: OPT\_BRIDGE\_DEV='no'

Mit 'yes' wird das Bridge Paket aktiviert, mit 'no' wird es deaktiviert.

**BRIDGE\_DEV\_BOOTDELAY** Default: BRIDGE\_DEV\_BOOTDELAY='yes'

Diese Einstellung ist optional und kann auch komplett weggelassen werden.

Da eine Bridge mindestens  $2 \times \text{BRIDGE\_DEV\_x\_FORWARD\_DELAY}$  in Sekunden an Zeit benötigt, um aktiv zu werden, ist diese Zeitspanne abzuwarten, wenn die Devices beim Start von fli4l sofort benötigt werden, um z.B. Syslogmeldungen zu verschicken oder sich per DSL einzuwählen. Wird der Eintrag auf 'yes' gelassen wird automatisch  $2 \times \text{BRIDGE\_DEV\_x\_FORWARD\_DELAY}$  gewartet. Werden die Bridges nicht direkt beim Start benötigt, sollten Sie hier den Wert 'no' eintragen um den Startvorgang des fli4l-Routers zu beschleunigen.

**BRIDGE\_DEV\_N** Default: BRIDGE\_DEV\_N='1'

Die Anzahl der voneinander unabhängigen Bridges. Jede Bridge ist von den anderen vollkommen isoliert zu betrachten. Das gilt insbesondere für die Einstellung von BRIDGE\_DEV\_x\_STP. Es wird pro Bridge ein virtuelles Device mit Namen 'br<nummer>' angelegt.

**BRIDGE\_DEV\_x\_NAME** Default: BRIDGE\_DEV\_x\_NAME=""

Der symbolische Name der Bridge. Dieser Name kann von anderen Paketen benutzt werden um die Bridge unabhängig von dem Gerätenamen zu benutzen.

**BRIDGE\_DEV\_x\_DEVNAME** Default: BRIDGE\_DEV\_x\_DEVNAME=""

Jedes Bridgegerät braucht einen Namen in der Form von 'br<nummer>'. Dabei darf <nummer> eine Zahl zwischen '0' und '99' ohne führende '0' sein. Mögliche Einträge sind also 'br0', 'br9' oder 'br42'. Die Namen können beliebig gewählt werden, die erste Bridge kann also 'br3' heissen und die zweite 'br0'.

**BRIDGE\_DEV\_x\_DEV\_N** Default: BRIDGE\_DEV\_x\_DEV\_N='0'

Wie viele Netzwerkgeräte gehören der Bridge an? Die Anzahl der Devices, die fest an die Bridge gebunden werden sollen. Kann auch '0' sein, wenn die Bridge nur als Platzhalter für eine IP-Adresse sein soll, die dann von einem an die Bridge gebundenen VPN-Tunnel übernommen werden soll.

**BRIDGE\_DEV\_x\_DEV\_x\_DEV** Gibt an, welches Device an die Bridge gehängt werden kann. hier kann ein eth-Device (z.B. 'eth0'), ein Bonding-Device (z.B. 'bond0') oder auch ein Vlan-Device eingetragen werden (z.B. 'vlan11'). Ein hier eingebundenes Device darf nicht mehr an anderer Stelle verwendet werden und auch keine IP erhalten.

```
BRIDGE_DEV_1_DEV_N='3'
BRIDGE_DEV_1_DEV_1_DEV='eth0.11' #VLAN 11 auf eth0
BRIDGE_DEV_1_DEV_2_DEV='eth2'
BRIDGE_DEV_1_DEV_3_DEV='bond0'
```



**BRIDGE\_DEV\_x\_AGING** Default: `BRIDGE_DEV_x_AGING='300'`

Diese Einstellung ist optional und kann auch komplett weggelassen werden.

Gibt an nach welcher Zeit alte Einträge in der MAC Tabelle der Bridge gelöscht werden. Wenn die hier angegebene Zeit in Sekunden keine Daten von dem Rechner mit der Netzwerkkarte empfangen oder verschickt worden sind wird diese entsprechende MAC Adresse aus der Bridge MAC Tabelle entfernt.

**BRIDGE\_DEV\_x\_GARBAGE\_COLLECTION\_INTERVAL** Default: `BRIDGE_DEV_x_GARBAGE_COLLECTION_INTERVAL='300'`

Diese Einstellung ist optional und kann auch komplett weggelassen werden.

Gibt an nach wieviel Sekunden eine „Müllsammlung“ gemacht wird. Dabei werden alle dynamischen Einträge der Bridge auf ihre Gültigkeit geprüft und veraltete oder nicht mehr gültige Einträge entfernt. Insbesondere bedeutet dies, dass alte nicht mehr gültige Verbindungen entfernt werden.

**BRIDGE\_DEV\_x\_STP** Default: `BRIDGE_DEV_x_STP='no'`

Diese Einstellung ist optional und kann auch komplett weggelassen werden.

Das Spanning Tree Protokoll erlaubt es, mehrere Verbindungen zu anderen Switches zu unterhalten. Dadurch wird eine Redundanz erzielt, die die Funktionsfähigkeit des Netzwerkes im Falle eines Ausfalls einer Leitung gewährleistet. Ohne den Einsatz von STP sind redundante Leitungen zwischen Switches nicht möglich, das Netzwerk würde nicht funktionieren. Das STP versucht immer die schnellstmögliche Verbindung zwischen zwei Switches zu benutzen, so dass auch der Einsatz von zwei unterschiedlich schnellen Leitungen sinnvoll ist. So könnte man z.B. eine 1 Gbit/s Verbindung als Hauptverbindung benutzen und eine zweite 100 Mbit/s Verbindung als Sicherheit.

Einen guten Artikel mit einigen Hintergrundinformationen finden Sie auf dieser Seite: [http://de.wikipedia.org/wiki/Spanning\\_Tree\\_Protocol](http://de.wikipedia.org/wiki/Spanning_Tree_Protocol).

**BRIDGE\_DEV\_x\_PRIORITY** Default: `BRIDGE_DEV_x_PRIORITY='0'`

Diese Einstellung ist optional und kann auch komplett weggelassen werden.

Nur gültig wenn `BRIDGE_DEV_x_STP='yes'` gesetzt wird!

Welche Priorität hat diese Bridge? Die Bridge mit der geringsten Priorität in der aktuellen Landschaft gewinnt die Wahl zur Hauptbridge. Jede Bridge sollte eine unterschiedliche Priorität haben. Bitte beachten Sie, dass die Bridge mit der geringsten Priorität auch über die größte Bandbreite verfügen sollte, da diese alle 2 Sekunden (oder die unter `BRIDGE_DEV_x_HELLO`) Steuerpakete verschickt und auch der gesamte restliche Datenverkehr über sie abgewickelt wird.

Gültige Werte sind '0' bis '61440' in Schritten von 4096.

**BRIDGE\_DEV\_x\_FORWARD\_DELAY** Default: `BRIDGE_DEV_x_FORWARD_DELAY='15'`

Diese Einstellung ist optional und kann auch komplett weggelassen werden.

Nur gültig wenn `BRIDGE_DEV_x_STP='yes'` gesetzt wird!

Wenn ein Bridgeanschluß deaktiviert war und erneut aktiviert werden soll, oder auch wenn der Anschluß gerade neu zur Bridge hinzugekommen ist, dauert es die angegebene

Zeitspanne (in Sekunden)  $\times 2$  bis der Anschluß Daten weiterleiten kann. Dieser Parameter ist maßgebend für die Dauer, die die Bridge benötigt um einer toten Verbindung zu erkennen. Die Zeitspanne wird nach folgender Formel in Sekunden berechnet:

$$\text{BRIDGE\_DEV\_x\_MAX\_MESSAGE\_AGE} + (2 \times \text{BRIDGE\_DEV\_x\_FORWARD\_DELAY})$$

Daraus ergibt sich mit den Standardwerten:  $20 + (2 \times 15) = 50$  Sekunden. Die Zeit bis eine tote Verbindung erkannt wird kann minimiert werden, wenn `BRIDGE_DEV_x_HELLO` auf 1 Sekunde und die `BRIDGE_DEV_x_FORWARD_DELAY` auf 4 Sekunden gestellt wird. Zusätzlich muss `BRIDGE_DEV_x_MAX_MESSAGE_AGE` auf 4 Sekunden eingestellt werden. Daraus ergibt sich folgender Wert:  $4 + (2 \times 4) = 12$  Sekunden. Schneller geht es nicht.

**BRIDGE\_DEV\_x\_HELLO** Default: `BRIDGE_DEV_x_HELLO='2'`

Diese Einstellung ist optional und kann auch komplett weggelassen werden.

Nur gültig wenn `BRIDGE_DEV_x_STP='yes'` gesetzt wird!

Die mit `BRIDGE_DEV_x_HELLO` angegebene Zeit ist der Zeitabstand in Sekunden, in dem die sogenannten Hello Nachrichten von der Hauptbridge verschickt werden. Diese Nachrichten sind für die automatische Konfiguration von STP notwendig.

**BRIDGE\_DEV\_x\_MAX\_MESSAGE\_AGE** Default: `BRIDGE_DEV_x_MAX_MESSAGE_AGE='20'`

Diese Einstellung ist optional und kann auch komplett weggelassen werden.

Nur gültig wenn `BRIDGE_DEV_x_STP='yes'` gesetzt wird!

Die maximale Gültigkeitsdauer der letzten Hello Nachricht. Wenn innerhalb dieser Zeit (in Sekunden) keine neue Hello Nachricht empfangen wird, wird eine neue Wahl der Hauptbridge ausgelöst. Deshalb darf dieser Wert **nie** kleiner als  $2 \times \text{BRIDGE\_DEV\_x\_HELLO}$  sein.

**BRIDGE\_DEV\_x\_DEV\_x\_PORT\_PRIORITY** Default: `BRIDGE_DEV_x_DEV_x_PORT_PRIORITY='128'`

Diese Einstellung ist optional und kann auch komplett weggelassen werden.

Nur gültig wenn `BRIDGE_DEV_x_STP='yes'` gesetzt wird!

Ist nur relevant, wenn mehrere Verbindungen mit der selben `BRIDGE_DEV_x_DEV_x_PATHCOST` zum selben Ziel führen. Ist dies der Fall wird die Verbindung mit der geringsten Priorität ausgewählt.

Gültige Werte sind '0' bis '240' in Schritten von '16'.

**BRIDGE\_DEV\_x\_DEV\_x\_PATHCOST** Default: `BRIDGE_DEV_x_DEV_x_PATHCOST='100'`

Diese Einstellung ist optional und kann auch komplett weggelassen werden.

Nur gültig wenn `BRIDGE_DEV_x_STP='yes'` gesetzt wird!

Bestimmt indirekt die Bandbreite für diese Verbindung. Je geringer der Wert, desto höher ist die Bandbreite und damit wird die Verbindung höher priorisiert.

Die vorgeschlagene Berechnungsgrundlage ist 1000000 / kbit/s, was zu den in Tabelle 4.3 aufgelisteten Werten führt. Bitte beachten Sie, dass bei der Berechnung die tatsächlich nutzbare Bandbreite in die Formel eingesetzt werden muss. Dadurch ergeben sich vor allem für WLAN deutliche niedrigere Werte als man erwarten würde.

Hinweis: Der aktuelle IEEE Standard von 2004 benutzt für die Bandbreitenberechnung 32 Bitzahlen, die von Linux noch nicht unterstützt werden.

Bandbreite	Einstellung von BRIDGE_DEV_x_DEV_x_PATHCOST
64 kbit/s	15625
128 kbit/s	7812
256 kbit/s	3906
10 Mbit/s	100
11 Mbit/s	190
54 Mbit/s	33
100 Mbit/s	10
1 Gbit/s	1

Tabelle 4.3.: Werte für BRIDGE\_DEV\_x\_DEV\_x\_PATHCOST in Abhängigkeit von der Bandbreite

#### 4.3.6. Anmerkungen

Eine Bridge leitet jede Art von Ethernetdaten weiter - somit läßt sich z.B. auch ein normales DSL-Modem über WLAN ansprechen als hätte es eine WLAN Schnittstelle. Es wird kein Paket, welches die Bridge passiert auf irgendwelche unerwünschten Aktivitäten hin untersucht (das heisst der fli4l Paketfilter wird nicht aktiv!), wodurch der Einsatz z.B. als WLAN Access Point nur unter sorgfältiger Abwägung der Sicherheitsrisiken zu empfehlen ist. Es gibt allerdings auch die Möglichkeit die EBTables Unterstützung zu aktivieren.

#### 4.3.7. EBTables - EBTables für fli4l

Ab der Version 2.1.9 hat fli4l auch rudimentäre EBTables Unterstützung. Mit `OPT_EBTABLES='yes'` wird die EBTables Unterstützung aktiviert. Damit werden alle EBTables Kernelmodule geladen und das ebttables Programm auf dem fli4l-Router zur Verfügung gestellt. Im Gegensatz zur wesentlich vereinfachten Konfiguration des netfilter durch die verschiedenen Filterlisten von fli4l ist es notwendig selbstständig ein ebttables Skript zu schreiben. Das bedeutet, sie müssen das komplette ebttables Skript selbst schreiben.

Für Hintergrundinformationen zu der EBTables Unterstützung lesen sie bitte die Dokumentation auf der EBTables Homepage unter <http://ebtables.sourceforge.net>.

Es gibt die Möglichkeit ebttables Kommandos vor und nach dem Einrichten des netfilters (die `PF_INPUT_x`, `PF_FORWARD_x` usw) auf dem fli4l-Router abzusetzen. Legen Sie dazu je nach Bedarf im Verzeichnis `config/ebtables` die Dateien `ebtables.pre` und `ebtables.post` an. Die Datei `ebtables.pre` wird vor der Konfiguration des netfilters ausgeführt, die `ebtables.post` Datei danach. Bitte bedenken sie, dass ein Fehler in den ebttables Skripten unter Umständen den Startvorgang des fli4l-Routers unterbricht!

**Vor Einsatz der EBTables Unterstützung sollten sie unbedingt die komplette EBTables Dokumentation lesen. Durch den Einsatz von EBTables ändert sich das Verhalten des fli4l-Router unter Umständen! So funktioniert z.B. das mac: Filtern in der PF\_FORWARD nicht mehr wie gewohnt.**

Sehr interessant ist folgende Seite, die einen kleinen Einblick in die Funktionsweise der EBTables Unterstützung bringt: [http://ebtables.sourceforge.net/br\\_fw\\_ia/br\\_fw\\_ia.html](http://ebtables.sourceforge.net/br_fw_ia/br_fw_ia.html).

### 4.3.8. SWITCH - Switch-Konfiguration

Dieses OPT erlaubt es, einen im fli4l verbauten Hardware-Switch zu konfigurieren. Einige Plattformen wie der Banana Pi R-1 stellen mehrere Netzwerk-Ports bereit, die intern zu einem Switch zusammengefasst sind. Erst durch eine geeignete Switch-Konfiguration kann man die einzelnen Netzwerk-Ports (oder Gruppen davon) einzelnen Netzen (VLANs) zuordnen.

**OPT\_SWITCH** Diese Variable aktiviert die Switch-Konfiguration.

Standard-Einstellung: `OPT_SWITCH='no'`

Beispiel: `OPT_SWITCH='yes'`

**SWITCH\_N** Diese Variable gibt die Anzahl der Switch-Geräte an, die es zu konfigurieren gilt. Typischerweise ist nur ein Switch vorhanden.

Standard-Einstellung: `SWITCH_N='0'`

Beispiel: `SWITCH_N='1'`

**SWITCH\_x\_DEV** Hier wird die Netzwerk-Schnittstelle angegeben, hinter welcher der Switch steckt. Zu beachten ist, dass über eine `NET_DRV_x`-Variable der passende Switch-Treiber geladen sein muss. Beim Banana Pi R-1 ist dies `"b53_mdio.ko"`.

Beispiel: `SWITCH_1_DEV='eth0'`

**SWITCH\_x\_VLAN\_N** Hier wird die Anzahl der logischen Netze angegeben, in die der Switch partitioniert werden soll. Diese Netze werden intern im Switch durch VLANs abgebildet.

Beispiel: `SWITCH_1_VLAN_N='2'`

**SWITCH\_x\_VLAN\_y\_ID** Diese Variable enthält die ID des zu definierenden VLANs. Dieses VLAN muss durch das `VLAN-OPT` definiert werden, damit der fli4l-Router überhaupt Zugriff darauf hat.

Beispiel: `SWITCH_1_VLAN_1_ID='100'`

**SWITCH\_x\_VLAN\_y\_PORT\_N** Hier wird die Anzahl der Netzwerk-Ports angegeben, die Teil dieses VLANs werden sollen.

Beispiel: `SWITCH_1_VLAN_1_PORT_N='3'`

**SWITCH\_x\_VLAN\_y\_PORT\_z\_ID** Diese Variable enthält die ID des zu verwendenden Netzwerk-Ports. Diese IDs sind Hardware-spezifisch und können i. d. R. nicht allgemein abgeleitet werden. Der Banana Pi R-1 nummeriert seine Ports folgendermaßen von links nach rechts: 2 1 0 4 3.

Beispiel:

```
SWITCH_1_VLAN_1_PORT_1_ID='0'
SWITCH_1_VLAN_1_PORT_2_ID='1'
SWITCH_1_VLAN_1_PORT_3_ID='2'
```

**SWITCH\_x\_VLAN\_y\_PORT\_z\_MODE** Hier wird angegeben, ob der Port bei Netzwerk-Paketen dieses (!) VLANs die VLAN-Kennung entfernen (Modus “untagged”) oder beibehalten (Modus “tagged”) soll. In der Regel will man die VLAN-Kennungen entfernen, damit die angeschlossenen Endgeräte keine Kenntnisse über die konfigurierten VLANs haben müssen.

Zu beachten ist, dass ein Netzwerk-Port höchstens für *ein* VLAN als “untagged” konfiguriert werden kann, da sonst eine VLAN-Zuordnung bei hereinkommenden ungetaggten Netzwerk-Paketen nicht mehr möglich ist. Hingegen kann ein Netzwerk-Port zusätzlich (oder ausschließlich) in mehreren VLANs als “tagged” konfiguriert sein.

Beispiel:

```
SWITCH_1_VLAN_1_PORT_1_MODE='untagged'
SWITCH_1_VLAN_1_PORT_2_MODE='untagged'
SWITCH_1_VLAN_1_PORT_3_MODE='untagged'
```

### Anwendungsbeispiel

Die folgende Konfiguration für den Banana Pi R-1 erstellt drei logische Netzwerke. Die ersten beiden Ports bilden VLAN 100, die nächsten beiden VLAN 101. Der fünfte Port ist der WAN-Port und einziger Port von VLAN 102. Alle Netzwerk-Ports arbeiten im “untagged”-Modus, da die VLANs nur intern für die Zuordnung der Pakete benutzt werden.

```
NET_DRV_N='1'
NET_DRV_1='b53_mdio'
NET_DRV_1_OPTION=''
[...]
OPT_VLAN_DEV='yes'
VLAN_DEV_N='3'
VLAN_DEV_1_DEV='eth0'
VLAN_DEV_1_VID='100'
VLAN_DEV_2_DEV='eth0'
VLAN_DEV_2_VID='101'
VLAN_DEV_3_DEV='eth0'
VLAN_DEV_3_VID='102'
[...]
OPT_SWITCH='yes'
SWITCH_N='1'
SWITCH_1_DEV='eth0'
SWITCH_1_VLAN_N='3'
SWITCH_1_VLAN_1_ID='100'
SWITCH_1_VLAN_1_PORT_N='2'
SWITCH_1_VLAN_1_PORT_1_ID='2'
SWITCH_1_VLAN_1_PORT_1_MODE='untagged'
SWITCH_1_VLAN_1_PORT_2_ID='1'
SWITCH_1_VLAN_1_PORT_2_MODE='untagged'
SWITCH_1_VLAN_2_ID='101'
SWITCH_1_VLAN_2_PORT_N='2'
SWITCH_1_VLAN_2_PORT_1_ID='0'
SWITCH_1_VLAN_2_PORT_1_MODE='untagged'
SWITCH_1_VLAN_2_PORT_2_ID='4'
```

```
SWITCH_1_VLAN_2_PORT_2_MODE='untagged'
SWITCH_1_VLAN_3_ID='102'
SWITCH_1_VLAN_3_PORT_N='1'
SWITCH_1_VLAN_3_PORT_1_ID='3'
SWITCH_1_VLAN_3_PORT_1_MODE='untagged'
```

#### 4.3.9. ETHTOOL - Einstellungen für Ethernet-Netzwerkadapter

Mit `OPT_ETHTOOL='yes'` wird das `ethtool`-Programm mit auf den fli4l kopiert und stellt es so zur Nutzung durch andere Pakete zu Verfügung. Mit Hilfe dieses Programms können diverse Einstellungen von Ethernet-Netzwerkkarten und -treibern angezeigt und verändert werden.

**ETHTOOL\_DEV\_N** Hier kann die Anzahl der Einstellungen angegeben werden, die beim Booten gesetzt werden.

Default: `ETHTOOL_DEV_N='0'`

**ETHTOOL\_DEV\_x** `ETHTOOL_DEV_x` gibt an, für welches Netzwerkgerät die Einstellung gelten soll.

Beispiel: `ETHTOOL_DEV_1='eth0'`

**ETHTOOL\_DEV\_x\_OPTION\_N** `ETHTOOL_DEV_x_OPTION_N` gibt die Anzahl der Einstellungen für das Gerät an.

**ETHTOOL\_DEV\_x\_OPTION\_x\_NAME**

**ETHTOOL\_DEV\_x\_OPTION\_x\_VALUE** Die Variable `ETHTOOL_DEV_x_OPTION_x_NAME` gibt den Namen und `ETHTOOL_DEV_x_OPTION_x_VALUE` den Wert für die zu ändernde Einstellung an.

Hier ist eine Liste der Optionen und möglichen Werte, die zur Zeit aktiviert sind:

- speed 10|100|1000|2500|10000 jeweils erweiterbar mit HD oder FD (default FD = Full-Duplex)
- autoneg on|off
- advertise %x
- wol p|u|m|b|a|g|s|d

Beispiel:

```
OPT_ETHTOOL='yes'
ETHTOOL_DEV_N='2'
ETHTOOL_DEV_1='eth0'
ETHTOOL_DEV_1_OPTION_N='1'
ETHTOOL_DEV_1_OPTION_1_NAME='wol'
ETHTOOL_DEV_1_OPTION_1_VALUE='g'
ETHTOOL_DEV_2='eth1'
ETHTOOL_DEV_2_OPTION_N='2'
ETHTOOL_DEV_2_OPTION_1_NAME='wol'
ETHTOOL_DEV_2_OPTION_1_VALUE='g'
ETHTOOL_DEV_2_OPTION_2_NAME='speed'
ETHTOOL_DEV_2_OPTION_2_VALUE='100hd'
```

Für nähere Informationen ist die Dokumentation von ethtool zu Rate zu ziehen: <http://linux.die.net/man/8/ethtool>

### 4.3.10. Beispiel

Für das Verständnis ist ein einfaches Beispiel sicher hilfreich. Wir gehen in unserem Beispiel von 2 Gebäudeteile aus, die mit 2 x 100 Mbit/s Verbindungen verbunden sind. Es sollen darüber 4 getrennte Netze von einem Gebäude in das andere geroutet werden.

Um dies zu verwirklichen, bietet sich eine Kombination aus Bonding (die 2 vorhandenen 100 Mbit/s Verbindungen in deren Übertragungsleistung zusammenfassen), VLAN (um mehrere getrennte Netze auf einer zusammengefassten Leitung transportieren zu können) und Bridging (um die Netze in den Gebäuden in das Bond/VLAN Gebilde einhängen zu können. (erfolgreich getestet mit 2x Intel e100 Karten und 1x Adaptec 4-Port Karte ANA6944.) Die beiden e100 haben in diesem Beispiel die Gerätenamen 'eth0' und 'eth1' und werden für die Gebäudeverbindung verwendet. Aktuell sind uns keine anderen Kartentypen außer die Intel e100 bekannt, die reibungslos mit VLAN zusammenarbeiten. Gigabit-Karten sollten aber prinzipiell auch funktionieren. Die 4 Anschlüsse der Multiportkarte dienen für die jeweiligen Netzwerke und haben die Gerätenamen 'eth2' bis 'eth5'.

Zuerst werden die beiden 100 Mbit/s Strecken gebondet:

```
OPT_BONDING_DEV='yes'
BONDING_DEV_N='1'
BONDING_DEV_1_DEVNAME='bond0'
BONDING_DEV_1_MODE='balance-rr'
BONDING_DEV_1_DEV_N='2'
BONDING_DEV_1_DEV_1='eth0'
BONDING_DEV_1_DEV_2='eth1'
```

Dadurch wird das Gerät 'bond0' erzeugt. Auf diese Bondingverbindung werden jetzt die VLANs aufgebaut, wir verwenden im Beispiel die VLAN-IDs 11, 22, 33 und 44:

```
OPT_VLAN_DEV='yes'
VLAN_DEV_N='4'
VLAN_DEV_1_DEV='bond0'
VLAN_DEV_1_VID='11'
VLAN_DEV_2_DEV='bond0'
VLAN_DEV_2_VID='22'
VLAN_DEV_3_DEV='bond0'
VLAN_DEV_3_VID='33'
VLAN_DEV_4_DEV='bond0'
VLAN_DEV_4_VID='44'
```

Und über diese VLAN Verbindungen wird nun eine Bridge in die einzelnen Netzwerksegmente gelegt. Ein Routing ist somit nicht notwendig.

```
OPT_BRIDGE_DEV='yes'
BRIDGE_DEV_N='4'
BRIDGE_DEV_1_NAME='_VLAN11_'
BRIDGE_DEV_1_DEVNAME='br11'
BRIDGE_DEV_1_DEV_N='2'
BRIDGE_DEV_1_DEV_1='bond0.11'
```

```
BRIDGE_DEV_1_DEV_2='eth2'  
BRIDGE_DEV_2_NAME='_VLAN22_'  
BRIDGE_DEV_2_DEVNAME='br22'  
BRIDGE_DEV_2_DEV_N='2'  
BRIDGE_DEV_2_DEV_1='bond0.22'  
BRIDGE_DEV_2_DEV_2='eth3'  
BRIDGE_DEV_3_NAME='_VLAN33_'  
BRIDGE_DEV_3_DEVNAME='br33'  
BRIDGE_DEV_3_DEV_N='2'  
BRIDGE_DEV_3_DEV_1='bond0.33'  
BRIDGE_DEV_3_DEV_2='eth4'  
BRIDGE_DEV_4_NAME='_VLAN44_'  
BRIDGE_DEV_4_DEVNAME='br44'  
BRIDGE_DEV_4_DEV_N='2'  
BRIDGE_DEV_4_DEV_1='bond0.44'  
BRIDGE_DEV_4_DEV_2='eth5'
```

Damit sind jetzt alle 4 Netze vollkommen transparent miteinander verbunden und teilen sich die 200 Mbit/s Verbindung. Selbst bei Ausfall einer 100 Mbit/s Verbindung funktioniert die Verbindung noch. Bei Bedarf kann auch noch die EBTablesunterstützung aktiviert werden um z.B. bestimmte Paketfilter zu aktivieren.

Diese Konfiguration wird auf zwei fli4l-Routern eingerichtet. Ich denke dieses Beispiel zeigt eindrucksvoll welche Möglichkeiten das advanced\_networking Paket ermöglicht.

### 4.4. CERT - Zertifikatsverwaltung

Das Paket CERT dient der Verwaltung von Zertifikaten auf dem fli4l. Zur Zeit beschränkt sich das Paket darauf, die nötigen TLS-Wurzelzertifikate auf den fli4l zu bringen, um via TLS gesicherte HTTP-Verbindungen auf dem fli4l aufbauen zu können. Dies wird beispielsweise vom DYNDNS-Paket benötigt, weil einige Schnittstellen zum Aktualisieren der externen IP-Adresse zwingend eine gesicherte HTTP-Verbindung erfordern.

**OPT\_CERT** Diese Option aktiviert die Zertifikatsverwaltung.

Standard-Einstellung: OPT\_CERT='no'

Beispiel: OPT\_CERT='yes'

**OPT\_CERT\_X509** Diese Option aktiviert die Verwaltung von X.509-Zertifikaten.

**Wichtig:** Beachten Sie, dass Sie auch OPT\_OPENSSL='yes' im TOOLS-Paket aktivieren müssen.

Standard-Einstellung: OPT\_CERT\_X509='no'

Beispiel: OPT\_CERT\_X509='yes'

**CERT\_X509\_MOZILLA** Mit dieser Variable kann die X.509-Zertifikatssammlung installiert werden, die mit dem Mozilla Firefox-Browser ausgeliefert wird. Sie kann folglich nur zusammen mit OPT\_CERT\_X509='yes' verwendet werden.

Standard-Einstellung: CERT\_X509\_MOZILLA='no'

Beispiel: CERT\_X509\_MOZILLA='yes'



## 4.5. CHRONY - Network Time Protocol Server/Client

OPT\_CHRONY erweitert fli4l um das [Network Time Protocol](#) (Seite 130) (NTP). Dies ist nicht mit dem *normalen* Time Protokoll zu verwechseln, welches das alte OPT\_TIME bereitstellt. Die Protokolle sind nicht kompatibel und somit werden gegebenenfalls neue Client-Programme, die NTP beherrschen, benötigt. Falls man nicht auf das einfache Time Protokoll verzichten kann, so läßt sich dieses Protokoll zusätzlich aktivieren.

OPT\_CHRONY arbeitet sowohl im Server, als auch im Client Modus. In der Funktion des Client gleicht es die Zeit des fli4l mit Zeitreferenzen (Time Server) im Internet ab. In der Grundeinstellung nutzt OPT\_CHRONY bis zu drei verschiedene Time Server aus dem Fundus von [pool.ntp.org](#) (Seite 131). Es ist jedoch auch möglich, über die Konfigurationsdatei eine andere Auswahl an Time Servern zu treffen. So ist es beispielsweise sinnvoll Server aus Europa zu wählen. Möglich ist das, indem man als Server `de.pool.ntp.org` angibt, wenn der Router bzw. der Provider in Deutschland ist. Weitere Informationen dazu auf der Webseite von [pool.ntp.org](#) (Seite 131).

In der Funktion des Server dient OPT\_CHRONY als Zeitreferenz für das lokale Netzwerk (LAN). NTP arbeitet auf Port 123.

Chrony zeichnet sich dadurch aus, dass es keine fortlaufende Verbindung zum Internet benötigt. Sobald die Verbindung getrennt wird (offline), erhält chrony hiervon Kenntnis und stellt den Zeitabgleich mit den Internet Time Servern ein. Somit löst chrony keinen neuen Verbindungsaufbau aus. Weiterhin verhindert chrony nicht die automatische Verbindungsunterbrechung, falls die HUP\_TIMEOUT, also die Zeit, in der keine Daten mit dem Internet ausgetauscht werden, erreicht wurde.

Damit der Zeitabgleich reibungslos funktioniert, sollte folgendes beachtet werden:

- Chrony erwartet, dass die BIOS-Uhr in der Zeitzone UTC läuft.  
UTC = Deutsche Zeit minus 1 (Winter) bzw. 2 (Sommer) Stunde(n)
- Seit der Version 2.1.12 setzt Chrony die Uhrzeit mit der ersten Verbindung zum Internet korrekt, auch wenn der Zeitunterschied sehr groß sein sollte (beispielsweise bei defekter Mainboardbatterie).
- Sollte das BIOS Jahreszahlen nach 1999 nicht richtig darstellen können (Year 2000 Bug) bzw. die Implementation der BIOS Uhr fehlerhaft sein, so muß `OPT_Y2K='yes'` (Seite 107) aktiviert werden!

Es können nur Time Server im Internet über die Default Route (0.0.0.0/0) erreicht werden, da nur die Default Route Chrony in den online Zustand versetzt. Ist der Router als LAN-Router konfiguriert, also keine DSL oder ISDN Circuits definiert, ist Chrony permanent im online Zustand.

**Disclaimer:** *Der Autor gibt weder eine Garantie auf die Funktionsfähigkeit des OPT\_CHRONY, noch haftet er für Schäden, z.B. Datenverlust, die durch den Einsatz von OPT\_CHRONY entstehen.*

### 4.5.1. Konfiguration des OPT\_CHRONY

Die Konfiguration erfolgt, wie bei allen fli4l Opts, durch Anpassung der Datei `Pfad/fli4l-4.0.0-trunk-rpi-r60784/<config>/chrony.txt` an die eigenen Anforderungen. Je-

doch sind fast alle Variablen des `OPT_CHRONY` optional. Optional heißt, die Variablen können, müssen aber nicht in der Konfigurationsdatei auftauchen. Somit ist die `chrony` Konfigurationsdatei im Auslieferungszustand fast leer und die optionalen Variablen sind sinnvoll vorbelegt. Möchte man dennoch eine anderen Konfiguration, müssen die Variablen von Hand eingefügt werden. Im weiteren erfolgt nun die Beschreibung der einzelnen Variablen:

### **OPT\_CHRONY** Default: `OPT_CHRONY='no'`

Die Einstellung `'no'` deaktiviert das `OPT_CHRONY` vollständig. Es werden keine Änderungen an dem `fl4l` Bootmedium bzw. dem Archiv `opt.img` vorgenommen. Weiter überschreibt das `OPT_CHRONY` grundsätzlich keine anderen Teile der `fl4l` Installation, mit einer Ausnahme. Es wird die Filterdatei ausgetauscht, die dafür sorgt, das Anfragen von außen nicht als Traffic gewertet werden (`fl4l` legt sicher nach Erreichen der Hangup Time auf). Die neue Filterdatei legt fest, dass der `chrony`-Traffic ebenfalls nicht mitgezählt wird, somit legt der Router weiterhin sicher auf.

Um `OPT_CHRONY` zu aktivieren, ist die Variable `OPT_CHRONY` auf `'yes'` zu setzen.

### **CHRONY\_TIMESERVICE** Default: `CHRONY_TIMESERVICE='no'`

Mit `CHRONY_TIMESERVICE` kann ein weiteres Protokoll zur Zeitübermittlung aktiviert werden. Dieses ist nur dann nötig, wenn die lokalen Rechner nicht mit NTP arbeiten können. Das zusätzliche Protokoll ist RFC 868 konform und arbeitet auf Port 37. Wenn immer möglich, sollte NTP vorgezogen werden.

Einen herzlichen Dank an Christoph Schulz, der das Programm `srv868` beigesteuert hat.

### **CHRONY\_TIMESERVER\_N** Default: `CHRONY_TIMESERVER_N='3'`

`CHRONY_TIMESERVER_N` legt die Anzahl der als Referenz benutzten Time Server fest. Der Anzahl entsprechend sind `CHRONY_TIMESERVER_x` Variablen anzulegen. Der Index `x` muß fortlaufend bis zur Gesamtanzahl heraufgezählt werden.

In der Grundeinstellung nutzt `chrony` drei Internet Time Server aus dem Fundus von [pool.ntp.org](http://pool.ntp.org) (Seite 131).

### **CHRONY\_TIMESERVER\_x** Default: `CHRONY_TIMESERVER_x='pool.ntp.org'`

Mit `CHRONY_TIMESERVER_x` kann eine eigene Liste von Internet Time Servern angelegt werden. Die Time Server können sowohl durch ihre IP als auch über ihren DNS Namen spezifiziert werden.

### **CHRONY\_LOG** Default: `CHRONY_LOG='/var/log/chrony'`

`CHRONY_LOG` bezeichnet das Verzeichnis, in dem `chrony` NTP-Messwerte und Informationen über vorgenommene Zeitkorrekturen ablegt.

## 4.5.2. Support

Support wird nur im Rahmen der [fl4l Newsgroups](#) (Seite 131) geleistet.

## 4.5.3. Literatur

Homepage von `chrony`: <http://chrony.tuxfamily.org/>

NTP: The Network Time Protocol: <http://www.ntp.org/>

pool.ntp.org: public ntp time server for everyone: <http://www.pool.ntp.org/de/>  
RFC 1305 - Network Time Protocol (Version 3) Specification, Implementation:  
<http://www.faqs.org/rfcs/rfc1305.html>  
fli4l Newsgroups und ihre Spielregeln: <http://www.fli4l.de/hilfe/newsgruppen/>

## 4.6. DNS\_DHCP - Dienste rund um DNS und DHCP

### 4.6.1. Hostnamen

#### Hosts

**OPT\_HOSTS** Mit der optionalen Variable OPT\_HOSTS kann die Konfiguration von Hostname deaktiviert werden!

**HOST\_N HOST\_x\_{attribute}** Es sollten alle Rechner im LAN beschrieben werden - mit IP-Adresse, Namen, Aliasnamen und evtl. Mac-Adressen für die dhcp-Konfiguration . Dazu setzt man zunächst die Anzahl der Rechner mit der Variablen HOST\_N.

**Hinweis:** Seit Version 3.4.0 wird der Eintrag für den Router aus den Angaben in der `<config>/base.txt` generiert. Sollen zusätzliche Aliasnamen aufgenommen werden, siehe auch [HOSTNAME\\_ALIAS\\_N](#) (Seite 83).

Anschließend werden mit den Attributen die Eigenschaften des Hostes definiert. Dabei sind einige Attribute Pflicht, wie z.B. IP-Adresse und Name, die anderen optional, d.h. man kann, aber man muß sie nicht spezifizieren.

**NAME** – Name des n-ten Hostes

**IP4** – IP-Adresse (ipv4) des n-ten Hostes

**IP6** – IP-Adresse (ipv6) des n-ten Hostes (optional). Wenn man “auto” verwendet, dann wird die Adresse bei aktiviertem OPT\_IPV6 aus einem IPv6-Präfix (mit /64er-Netzmaske) und der MAC-Adresse des jeweiligen Hosts automatisch berechnet. Damit das funktioniert, muss die MAC-Adresse via `HOST_x_MAC` gesetzt (siehe unten) und das Paket `ipv6` entsprechend konfiguriert werden.

**DOMAIN** – DNS-Domain des n-ten Hostes (optional)

**ALIAS\_N** – Anzahl der Alias-Namen des n-ten Hostes

**ALIAS\_m** – m-ter Alias-Name für den n-ten Host

**MAC** – Mac Adresse des n-ten Hostes

**DHCPTYP** – Vergabe der IP-Adresse per DHCP abhängig von MAC oder NAME (optional)

In der Beispiel-Datei sind 4 Rechner konfiguriert - nämlich die PCs “client1”, “client2”, “client3” und “client4”.

```
HOST_1_NAME='client1'           # 1st host: ip and name
HOST_1_IP4='192.168.6.1'
```

Aliasnamen müssen mit kompletter Domain angegeben werden.

## 4. Pakete

Die MAC-Adresse ist optional und ist nur dann relevant, wenn fli4l zusätzlich als DHCP-Server eingesetzt wird. Dies wird in der Beschreibung zum optionalen Programmpaket "OPT\_DHCP" erklärt, siehe unten. Ohne Einsatz als DHCP-Server sind lediglich die IP-Adresse, der Name des Rechners und eventuell Aliasnamen einzusetzen. Die MAC-Adresse ist eine 48-Bit-Adresse und besteht aus 6 Hex-Werten, welche durch einen Doppelpunkt voneinander getrennt werden, z.B.

```
HOST_2_MAC='de:ad:af:fe:07:19'
```

*Hinweis:* Wird fli4l um das IPv6-Paket ergänzt, brauchen keine IPv6-Adressen hinterlegt zu werden, wenn gleichzeitig die MAC-Adressen der Hosts vorliegen, weil das IPv6-Paket dann die IPv6-Adressen automatisch berechnet (modifiziertes EUI-64). Natürlich kann man aber den Automatismus unterbinden und feste IPv6-Adressen vorgeben, wenn man dies wünscht.

### Extra Hosts

#### HOST\_EXTRA\_N HOST\_EXTRA\_x\_NAME HOST\_EXTRA\_x\_IP4 HOST\_EXTRA\_x\_IP6

Mit diesen Variablen können weitere Hosts hinzugefügt werden die nicht der lokalen Domain angehören wie z.b. Hosts die sich auf der anderen Seite eines VPNs befinden.

### 4.6.2. DNS-Server

**OPT\_DNS** Um den DNS-Server zu aktivieren ist die Variable OPT\_DNS mit 'yes' zu belegen.

Werden im LAN keine Windows-Rechner verwendet oder ist bereits ein DNS-Server vorhanden, kann man OPT\_DNS auf 'no' setzen und den Rest in diesem Abschnitt übergehen.

Im Zweifel immer (Standard-Einstellung): OPT\_DNS='yes'

### Allgemeine DNS-Optionen

**DNS\_LISTEN\_N DNS\_LISTEN\_x** Wenn Sie OPT\_DNS='yes' gewählt haben, können Sie mit Hilfe von DNS\_LISTEN\_N die Anzahl, und mit DNS\_LISTEN\_1 bis DNS\_LISTEN\_N lokale IPs angeben, auf denen dnsmasq DNS-Anfragen annehmen darf. Sollten Sie bei DNS\_LISTEN\_N eine 0 eingetragen haben, beantwortet dnsmasq DNS-Anfragen auf allen lokalen IPs. An dieser Stelle dürfen nur IPs von existierenden Schnittstellen (ethernet, wlan ...) verwendet werden, es kommt sonst zu Warnmeldungen beim Start des Routers. Alternativ ist nun möglich hier auch ALIAS-Namen zu verwenden, z. B. IP\_NET\_1\_IPADDR

Für alle hier angegebenen Adressen werden bei PF\_INPUT\_ACCEPT\_DEF='yes' und/oder PF6\_INPUT\_ACCEPT\_DEF='yes' entsprechende ACCEPT-Regeln in der INPUT-Kette der Firewall erzeugt. Im Falle DNS\_LISTEN='0' werden ebenfalls Regeln erzeugt, die den DNS-Zugriff auf *allen* konfigurierten Schnittstellen erlauben.

**Wichtig:** Falls der DNS-Server auf zur Laufzeit dynamisch hinzugefügten Schnittstellen horchen soll, etwa auf Netzwerk-Schnittstellen von VPN-Tunneln, sollten Sie dieses Array leer lassen, da andernfalls der DNS-Server nicht auf DNS-Anfragen antworten wird, die über den VPN-Tunnel gestellt werden.

Im Zweifelsfalle können die Standardeinstellungen übernommen werden.

**DNS\_BIND\_INTERFACES** Falls Sie den DNS-Server via `DNS_LISTEN_x` nur an bestimmte Adressen binden möchten *und* zusätzlich einen *weiteren* DNS-Server an *andere* Adressen binden möchten, können Sie durch diese Option den DNS-Server anweisen, sich auch wirklich *nur* an die gelisteten Adressen zu binden. Standardmäßig bindet sich der DNS-Server an *alle* Schnittstellen und wirft bei Adressen im `DNS_LISTEN_x`-Array DNS-Anfragen, die an nicht konfigurierten Adressen ankommen, weg. Dies hat den Vorteil, dass der DNS-Server auch mit zur Laufzeit dynamisch hinzugefügten Schnittstellen umgehen kann, aber den Nachteil, dass kein alternativer DNS-Server auf dem Standard-DNS-Port 53 gleichzeitig laufen kann. Ein Anwendungsfall für einen zweiten DNS-Server ist, wenn Sie einen Slave-DNS-Server wie “yadifa” direkt auf dem fli4l-Router betreiben möchten. Soll also der dnsmasq nicht exklusiv auf dem fli4l eingesetzt werden, muss die Einstellung ‘yes’ gewählt und die für den dnsmasq zu nutzenden IP-Adressen per `DNS_LISTEN` konfiguriert werden.

**DNS\_VERBOSE** Logging von DNS-Queries: ‘yes’ oder ‘no’

Für ausführlichere Ausgaben des DNS, muß `DNS_VERBOSE` auf yes gesetzt werden. In diesem Fall werden DNS-Anfragen an den Nameserver protokolliert - und zwar über die syslog-Schnittstelle. Damit die Ausgaben auch sichtbar werden, ist dann auch die Variable `OPT_SYSLOGD='yes'` (Seite 105) zu setzen, s.u.

**DNS\_MX\_SERVER** Mit dieser Variable gibt man hier den Hostnamen für den MX-Record (Mail-Exchanger) für die in `DOMAIN_NAME` definierte Domain an. Ein MTA (Mail-Transport-Agent, wie z.B. sendmail) auf einem internen Server fragt per DNS nach einem Mail-Exchanger für die Zieldomain der zuzustellenden Mail. Der DNS-Server liefert hiermit dem MTA den entsprechenden Host, der für Mails der Domain `DOMAIN_NAME` zuständig ist.

**Dies ist keine automatische Konfiguration für Mail-Clients, wie z.B. Outlook! Also bitte nicht gmx.de hier eintragen und dann wundern, warum Outlook nicht funktioniert.**

**DNS\_FORBIDDEN\_N DNS\_FORBIDDEN\_x** Hier können Sie Domains angeben, bei denen DNS-Queries vom DNS-Server prinzipiell als “nicht vorhanden” beantwortet werden sollen.

Beispiel:

```
DNS_FORBIDDEN_N='1'
DNS_FORBIDDEN_1='foo.bar'
```

In diesem Fall wird zum Beispiel eine Anfrage nach `www.foo.bar` mit einem Fehler beantwortet.

Man kann damit auch ganze Top-Level-Domains verbieten:

```
DNS_FORBIDDEN_1='de'
```

Dann ist die Namensauflösung für sämtliche Rechner in der DE-Topleveldomain abgeschaltet.

**DNS\_REDIRECT\_N DNS\_REDIRECT\_x DNS\_REDIRECT\_x\_IP** Hier können Domains angegeben werden, bei welchen DNS-Queries vom DNS-Server auf eine spezielle IP umgeleitet werden.

Beispiel:

```
DNS_REDIRECT_N='1'  
DNS_REDIRECT_1='yourdom.dyndns.org'  
DNS_REDIRECT_1_IP='192.168.6.200'
```

In diesem Fall wird zum Beispiel eine Anfrage nach yourdom.dyndns.org mit der IP 192.168.6.200 beantwortet. Somit kann man externe Domains auf andere IPs umleiten.

**DNS\_BOGUS\_PRIV** Setzt man diese Variable auf 'yes', werden reverse-lookups für IP-Adressen nach RFC1918 (Private Address Bereiche) nicht vom dnsmasq an andere DNS-Server weitergeleitet, sondern vom dnsmasq beantwortet.

**DNS\_FORWARD\_PRIV\_x** Gelegentlich möchte man trotz aktiviertem DNS\_BOGUS\_PRIV die Auflösung von Adressen einiger privater Subnetze dennoch an die konfigurierten DNS-Server delegieren. Dies ist zum Beispiel nötig, wenn ein Uplink-Router private Subnetze verwaltet. Diese Array-Variable kann dafür genutzt werden, die privaten Subnetze zu benennen, deren Auflösung delegiert werden darf.

**DNS\_FILTERWIN2K** Setzt man diese Variable auf 'yes', werden DNS-Anfragen vom Typ SOA, SRV und ANY geblockt. Dienste, die diese Anfragen verwenden, werden dann nicht mehr ohne weitere Konfiguration funktionieren.

Dazu zählen zum Beispiel:

- XMPP (Jabber)
- SIP
- LDAP
- Kerberos
- Teamspeak3 (seit Client-Version 3.0.8)
- Minecraft (seit Vollversion 1.3.1)
- Ermittlung des Domänencontrollers (Win2k)

Siehe hierzu auch:

- Generelle Erklärung der DNS Record Arten:  
[http://en.wikipedia.org/wiki/List\\_of\\_DNS\\_record\\_types](http://en.wikipedia.org/wiki/List_of_DNS_record_types)
- Manpage von dnsmasq:  
<http://www.thekelleys.org.uk/dnsmasq/docs/dnsmasq-man.html>
- SRV-Record im Speziellen:  
[http://de.wikipedia.org/wiki/SRV\\_Resource\\_Record](http://de.wikipedia.org/wiki/SRV_Resource_Record)

Durch Setzen von 'no' können durch die zusätzlichen weitergeleiteten DNS-Anfragen ungewollte Einwahlverbindungen aufgebaut oder bestehende nicht

abgebaut werden. Insbesondere bei ISDN- und UMTS-Verbindungen können dadurch Mehrkosten entstehen. Sie müssen selbst abwägen, was für Sie wichtiger ist.

**DNS\_FORWARD\_LOCAL** setzt man diese Variable auf 'yes' kann der fli4l-Router in einer Domäne mit `DOMAIN_NAME='example.local'` konfiguriert werden, die wiederum per `DNS_ZONE_DELEGATION_x_DOMAIN='example.local'` von einem anderen Name-server aufgelöst wird.

**DNS\_LOCAL\_HOST\_CACHE\_TTL** Gibt die TTL (Time to live, in Sekunden) für Einträge aus den `/etc/hosts` Dateien und den per DHCP vergebenen IP-Adressen an. Der Standardwert für den fli4l-Router beträgt 60 Sekunden. Standardmäßig setzt der `dnsmasq` die TTL für lokale Einträge auf 0 und deaktiviert damit faktisch das nachfolgende Caching der DNS Einträge. Die Idee dahinter ist das ablaufende DHCP Leases usw. zeitnah weitergegeben werden können. Fragt allerdings z.B. ein lokaler IMAP Proxy die DNS Einträge dadurch mehrfach pro Sekunde ab ist das eine deutliche Belastung für das Netzwerk. Ein Kompromiss ist daher ein relativ kurzer TTL von 60 Sekunden. Es kann ja auch ohne die kurze TTL von 60 Sekunden jederzeit zu einem simplen abschalten eines Hosts kommen, so dass die abfragende Software sowieso mit nicht antwortenden Hosts klarkommen muss.

**DNS\_SUPPORT\_IPV6** (optional)

setzt man diese optionale Variable auf 'yes' wird die Unterstützung für IPV6- Adressen des DNS-Servers aktiviert.

### DNS-Zonenkonfiguration

Der `dnsmasq` kann auch eine DNS-Domäne eigenständig verwalten, d.h. er ist "authoritativ" für diese Domäne. Dazu muss man zweierlei tun: Zum einen muss angegeben werden, welcher externe (!) DNS-Namensdienst auf den eigenen fli4l verweist und über welche Netzwerkschnittstelle dies passiert. Die Angabe der externen Referenz ist erforderlich, denn die Domäne, welche der fli4l verwaltet, ist ja immer eine Unterdomäne einer anderen Domäne.<sup>2</sup> Die Angabe der Schnittstelle ist wichtig, weil sich der `dnsmasq` dort "nach außen" anders verhält als auf den anderen Schnittstellen "nach innen": Nach außen beantwortet der `dnsmasq` niemals Anfragen für Namen außerhalb der konfigurierten eigenen Domäne. Nach innen funktioniert der `dnsmasq` natürlich auch als DNS-Relay ins Internet, damit die Auflösung von nicht-lokalen Namen funktioniert.

Zum anderen muss konfiguriert werden, welche Netze nach außen via Namensauflösung erreichbar sind. Hierbei sollten natürlich nur Netze mit öffentlichen IP-Adressen angegeben werden, denn über private Adressen können Hosts von außen ohnehin nicht erreicht werden.

Im Folgenden wird die Konfiguration an einem Beispiel beschrieben. Dieses Beispiel setzt das IPv6-Paket sowie ein öffentlich geroutetes IPv6-Präfix voraus; letzteres kann z.B. von einem 6in4-Tunnel-Provider wie Hurricane Electric bereitgestellt werden.

**DNS\_AUTHORITATIVE** Die Einstellung `DNS_AUTHORITATIVE='yes'` aktiviert den authoritativen Modus des `dnsmasq`. Dies reicht jedoch nicht aus, da weitere Angaben gemacht werden müssen (s.u.).

---

<sup>2</sup>Wir gehen hier mal davon aus, dass niemand einen fli4l als DNS-Rootserver verwendet...

Standard-Einstellung: `DNS_AUTHORITATIVE='no'`

Beispiel: `DNS_AUTHORITATIVE='yes'`

**DNS\_AUTHORITATIVE\_NS** Mit dieser Variable wird der DNS-Name konfiguriert, über den auf den fli4l von außen mit Hilfe eines DNS-NS-Records verwiesen wird. Das kann auch ein DNS-Name sein, der zu einem Dynamic DNS-Dienst gehört.

Beispiel: `DNS_AUTHORITATIVE_NS='fli4l.noip.me'`

**DNS\_AUTHORITATIVE\_LISTEN** Mit dieser Variable wird konfiguriert, an welcher Adresse bzw. Schnittstelle der dnsmasq DNS-Anfragen für die eigene Domäne autoritativ beantwortet. Symbolische Namen wie `IP_NET_2_IPADDR`, `IP_NET_1_DEV` oder `{LAN}` sind erlaubt. Der dnsmasq kann nur an *einer* Adresse/Schnittstelle autoritativ antworten.

**Wichtig:** *Zu beachten ist, dass dies niemals eine Adresse/Schnittstelle sein darf, an der das eigene LAN hängt, weil sonst keine nicht-lokalen Namen mehr im LAN aufgelöst werden können!*

Beispiel: `DNS_AUTHORITATIVE_LISTEN='IP_NET_2_IPADDR'`

**DNS\_ZONE\_NETWORK\_N DNS\_ZONE\_NETWORK\_x** Hier werden die Netzadressen angegeben, für die der dnsmasq autoritativ die Namen auflösen soll. Dabei funktioniert sowohl die Vorwärts- (Name zu Adresse) als auch die Rückwärtsauflösung (Adresse zu Name).

Ein komplettes Beispiel:

```
DNS_AUTHORITATIVE='yes'
DNS_AUTHORITATIVE_NS='fli4l.noip.me'
DNS_AUTHORITATIVE_LISTEN='IP_NET_2_IPADDR' # Uplink hängt an eth1
DNS_ZONE_NETWORK_N='1'
DNS_ZONE_NETWORK_1='2001:db8:11:22::/64'   # lokales IPv6-LAN
```

Dabei wird angenommen, dass “2001:db8:11::/48” ein zu dem fli4l öffentlich geroutetes IPv6-Präfix ist und dass für das LAN das Subnetz 22 gewählt wurde.

### DNS Zone Delegation

**DNS\_ZONE\_DELEGATION\_N DNS\_ZONE\_DELEGATION\_x** Es gibt besondere Situationen, wo die Angabe eines oder mehrerer DNS Server sinnvoll ist, z.B. bei Einsatz von fli4l im Intranet ohne Internetanschluss oder einem Mix von diesen (Intranet mit eigenem DNS Server und zusätzlich Internetanschluss).

Stellen wir uns folgendes Szenario vor:

- Circuit 1: Einwahl in das Internet
- Circuit 2: Einwahl in das Firmen-Netz 192.168.1.0 (firma.de)

Dann wird man `ISDN_CIRC_1_ROUTE` auf ‘0.0.0.0’ und `ISDN_CIRC_2_ROUTE` auf ‘192.168.1.0’ setzen. Bei Zugriff auf Rechner mit IP-Adresse 192.168.1.x wird fli4l dann den Circuit 2, sonst den Circuit 1 benutzen. Wenn das Firmennetz aber nicht öffentlich ist, wird in



#### 4. Pakete

diesem vermutlich ein eigener DNS Server betrieben. Nehmen wir an, die Adresse dieses DNS Servers wäre 192.168.1.12 und der Domainname wäre "firma.de".

In diesem Fall gibt man an:

```
DNS_ZONE_DELEGATION_N='1'
DNS_ZONE_DELEGATION_1_UPSTREAM_SERVER_N='1'
DNS_ZONE_DELEGATION_1_UPSTREAM_SERVER_1_IP='192.168.1.12'
DNS_ZONE_DELEGATION_1_DOMAIN_N='1'
DNS_ZONE_DELEGATION_1_DOMAIN_1='firma.de'
```

Dann werden bei DNS Anfragen an die Domain firma.de der firmeninterne DNS Server benutzt. Alle anderen DNS Anfragen gehen wie üblich an die DNS Server im Internet.

Ein anderer Fall:

- Circuit 1: Internet
- Circuit 2: Firmen-Netz 192.168.1.0 \*mit\* Internetanschluss

Hier hat man also die Möglichkeit, auf 2 Wegen in das Internet zu gelangen. Möchte man geschäftliches und privates trennen, bietet sich dann folgendes an:

```
ISDN_CIRC_1_ROUTE='0.0.0.0'
ISDN_CIRC_2_ROUTE='0.0.0.0'
```

Man legt also auf beide Circuits eine Defaultroute und schaltet dann die Route mit dem imond-Client um - je nach Wunsch. Auch in diesem Fall sollte man DNS\_ZONE\_DELEGATION\_N und DNS\_ZONE\_DELEGATION\_x\_DOMAIN\_x wie oben beschrieben einstellen.

Möchte man auch die Reverse-DNS-Auflösung für ein so erreichbares Netz nutzen, z.B. wird ein Reverselookup von einigen Mailserver gemacht, gibt man in der optionalen Variable DNS\_ZONE\_DELEGATION\_x\_NETWORK\_x, das/die Netz(werke) an, für die der Reverselookup aktiviert werden soll. Das folgende Beispiel verdeutlicht das:

```
DNS_ZONE_DELEGATION_N='2'
DNS_ZONE_DELEGATION_1_UPSTREAM_SERVER_N='1'
DNS_ZONE_DELEGATION_1_UPSTREAM_SERVER_1_IP='192.168.1.12'
DNS_ZONE_DELEGATION_1_DOMAIN_N='1'
DNS_ZONE_DELEGATION_1_DOMAIN_1='firma.de'
DNS_ZONE_DELEGATION_1_NETWORK_N='1'
DNS_ZONE_DELEGATION_1_NETWORK_1='192.168.1.0/24'
DNS_ZONE_DELEGATION_2_UPSTREAM_SERVER_N='1'
DNS_ZONE_DELEGATION_2_UPSTREAM_SERVER_1_IP='192.168.2.12'
DNS_ZONE_DELEGATION_2_DOMAIN_N='1'
DNS_ZONE_DELEGATION_2_DOMAIN_1='bspfirma.de'
DNS_ZONE_DELEGATION_2_NETWORK_N='2'
DNS_ZONE_DELEGATION_2_NETWORK_1='192.168.2.0/24'
DNS_ZONE_DELEGATION_2_NETWORK_2='192.168.3.0/24'
```

Mit der Konfigurationsoption DNS\_ZONE\_DELEGATION\_x\_UPSTREAM\_SERVER\_x\_QUERYSOURCEIP kann man die IP-Adresse für die ausgehenden DNS Anfragen an den oder die Upstream

DNS Server setzen. Das ist z.B. dann sinnvoll wenn man den Upstream DNS Server über ein VPN erreicht und nicht möchte, dass die lokale VPN Adresse vom fli4l-Router als Quell IP-Adresse beim Upstream DNS Server auftaucht. Ein anderer Anwendungsfall ist eine vom Upstream DNS Server aus gesehen nicht routbare IP-Adresse (die durch ein VPN Interface evtl. auftritt). Auch in diesem Fall ist es notwendig die vom dnsmasq benutzte ausgehende IP-Adresse fest auf eine vom fli4l-Router benutzte und vom Upstream DNS Server aus erreichbar IP-Adresse zu setzen.

```
DNS_ZONE_DELEGATION_N='1'
DNS_ZONE_DELEGATION_1_UPSTREAM_SERVER_N='1'
DNS_ZONE_DELEGATION_1_UPSTREAM_SERVER_1_IP='192.168.1.12'
DNS_ZONE_DELEGATION_1_UPSTREAM_SERVER_1_QUERYSOURCEIP='192.168.0.254'
DNS_ZONE_DELEGATION_1_DOMAIN_N='1'
DNS_ZONE_DELEGATION_1_DOMAIN_1='firma.de'
DNS_ZONE_DELEGATION_1_NETWORK_N='1'
DNS_ZONE_DELEGATION_1_NETWORK_1='192.168.1.0/24'
```

**DNS\_REBINDOK\_N DNS\_REBINDOK\_x\_DOMAIN** Der Nameserver *dnsmasq* lehnt normalerweise Antworten anderer Nameserver ab, die IP-Adressen aus privaten Netzwerken enthalten. Er verhindert dadurch eine bestimmte Klasse von Angriffen auf das Netzwerk. Hat man allerdings eine Domain in einem Netzwerk mit privaten IP-Adressen und einen extra Nameserver, der für dieses Netz zuständig ist, liefert der genau die Antworten, die vom *dnsmasq* abgelehnt werden würden. Diese Domains kann man in **DNS\_REBINDOK\_x** auflisten, die entsprechenden Antworten auf Anfragen zu der Domain werden dann akzeptiert. Ein weiteres Beispiel für Nameserver, die private IP-Adressen als Antwort liefern, sind sogenannte “Real-Time Blacklist Server”. Ein Beispiel basierend auf diesen könnte wie folgt aussehen:

```
DNS_REBINDOK_N='8'
DNS_REBINDOK_1_DOMAIN='rfc-ignorant.org'
DNS_REBINDOK_2_DOMAIN='spamhaus.org'
DNS_REBINDOK_3_DOMAIN='ix.dnsbl.manitu.net'
DNS_REBINDOK_4_DOMAIN='multi.surbl.org'
DNS_REBINDOK_5_DOMAIN='list.dnswl.org'
DNS_REBINDOK_6_DOMAIN='bb.barracudacentral.org'
DNS_REBINDOK_7_DOMAIN='dnsbl.sorbs.net'
DNS_REBINDOK_8_DOMAIN='nospam.login-solutions.de'
```

#### 4.6.3. DHCP-Server

**OPT\_DHCP** Mit **OPT\_DHCP** kann man einstellen, ob der DHCP-Server aktiviert wird.

**DHCP\_TYPE** (optional)

Mit dieser Variable legt man fest, ob man die interne DHCP-Funktion des *dnsmasq* benutzt, oder ob man auf den externen ISC-DHCPD zurückgreifen will. Im Falle des ISC-DHCPD entfällt der Support für DDNS.

**DHCP\_VERBOSE** aktiviert zusätzliche DHCP-Ausgaben im log.

**DHCP\_LS\_TIME\_DYN** legt die standard Lease-Time für dynamisch vergebene IP-Adressen fest.

**DHCP\_MAX\_LS\_TIME\_DYN** legt die maximale Lease-Time für dynamisch vergebene IP-Adressen fest.

**DHCP\_LS\_TIME\_FIX** Standard Lease-Time für statisch zugeordnete IP-Adressen.

**DHCP\_MAX\_LS\_TIME\_FIX** legt die maximale Lease-Time für statisch zugeordnete IP-Adressen fest.

**DHCP\_LEASES\_DIR** legt das Verzeichnis für die Leases-Datei fest. Möglich ist die Angabe eines absoluten Pfades oder des Wertes *auto*. Bei Angabe von *auto* wird die lease-Datei im Unterverzeichnis *dhcp* des persistent-Verzeichnisses (siehe Base-Dokumentation) abgelegt.

**DHCP\_LEASES\_VOLATILE** Befindet sich das Verzeichnis für die *Leases* in der Ram-Disk (da der Router z.B. von CD oder einem anderen nicht schreibbaren Medium bootet), gibt der Router beim Booten eine Warnung wegen einer fehlenden *Lease*-Datei aus. Diese Warnung entfällt, wenn man **DHCP\_LEASES\_VOLATILE** auf *yes* setzt.

**DHCP\_DNS\_SERVERS** legt die Adressen der DNS-Server fest.

Mehrere DNS-Server können durch Leerzeichen getrennt angegeben werden. Diese Variable ist optional. Wird hier nichts eingetragen, oder die Variable weggelassen, wird die IP-Adresse des zugehörigen Netzes verwendet, wenn der DNS-Server auf dem Router aktiviert ist. Es ist auch möglich, diese Variable auf 'none' zu setzen. Dann wird kein DNS-Server übertragen. Diese Einstellung wird ggf. von **DHCP\_RANGE\_x\_DNS\_SERVERS** überschrieben.

**DHCP\_WINS\_SERVERS** legt die Adressen der WINS-Server fest.

Mehrere WINS-Server können durch Leerzeichen getrennt angegeben werden. Diese Variable ist optional. Wird hier nichts eingetragen, oder die Variable weggelassen, wird bei installiertem und aktiviertem WINS-Server die Adresse des WINS-Server des SAMBA-Paketes übernommen. Es ist auch möglich, diese Variable auf 'none' zu setzen. Dann wird kein WINS-Server übertragen. Diese Einstellung wird ggf. von **DHCP\_RANGE\_x\_WINS\_SERVERS** überschrieben.

**DHCP\_NTP\_SERVERS** legt die Adressen der NTP-Server fest.

Mehrere NTP-Server können durch Leerzeichen getrennt angegeben werden. Diese Variable ist optional. Wird hier nichts eingetragen, oder die Variable weggelassen, wird die IP-Adresse des zugehörigen Netzes verwendet, wenn ein Zeitserverpaket auf dem Router aktiviert ist. Es ist auch möglich, diese Variable auf 'none' zu setzen. Dann wird kein NTP-Server übertragen. Diese Einstellung wird ggf. von **DHCP\_RANGE\_x\_NTP\_SERVERS** überschrieben.

**DHCP\_OPTION\_WPAD** aktiviert oder deaktiviert die Übermittlung der DHCP-OPTION 252 (Web Proxy Autodiscovery Protocol) womit Browser automatisiert die Proxy-Einstellungen beziehen können. (siehe [http://de.wikipedia.org/wiki/Web\\_Proxy\\_Autodiscovery\\_Protocol](http://de.wikipedia.org/wiki/Web_Proxy_Autodiscovery_Protocol))

**DHCP\_OPTION\_WPAD\_URL** definiert die URL der wpad.dat Datei oder wird leer gelassen um eine leere Antwort an den anfragenden Browser zu schicken, wodurch dieser keine weiteren regelmäßigen Anfragen durchführt.

#### Lokale DHCP-Range

**DHCP\_RANGE\_N** Anzahl der DHCP-Ranges

**DHCP\_RANGE\_x\_NET** Referenz zu einem in IP\_NET\_x definiertem Netz

**DHCP\_RANGE\_x\_START** legt die erste zu vergebende IP-Adresse fest.

**DHCP\_RANGE\_x\_END** legt die letzte zu vergebende IP-Adresse fest. Die beiden Variablen DHCP\_RANGE\_x\_START und DHCP\_RANGE\_x\_END kann man auch leer lassen, es wird dann keine DHCP-Range angelegt und nur die weiteren Variablen genutzt, um einem Host der per MAC-Zuordnung seine DHCP-IP bezieht, die Werte der Variablen zu übergeben.

**DHCP\_RANGE\_x\_DNS\_DOMAIN** legt eine spezielle DNS-Domain für DHCP-Hosts dieser Range fest. Diese Variable ist optional. Wird hier nichts eingetragen, oder die Variable weggelassen, wird der Default DNS-Domain DOMAIN\_NAME verwendet.

**DHCP\_RANGE\_x\_DNS\_SERVERS** legt die Adressen der DNS-Server fest.

Mehrere DNS-Server können durch Leerzeichen getrennt angegeben werden. Diese Variable ist optional. Wird hier nichts eingetragen, oder die Variable weggelassen, wird die Einstellung aus [DHCP\\_DNS\\_SERVERS](#) verwendet. Es ist auch möglich, diese Variable auf 'none' zu setzen. Dann wird kein DNS-Server übertragen.

**DHCP\_RANGE\_x\_WINS\_SERVERS** legt die Adressen der WINS-Server fest.

Mehrere WINS-Server können durch Leerzeichen getrennt angegeben werden. Diese Variable ist optional. Wird hier nichts eingetragen, oder die Variable weggelassen, wird die Einstellung aus [DHCP\\_WINS\\_SERVERS](#) verwendet. Es ist auch möglich, diese Variable auf 'none' zu setzen. Dann wird kein WINS-Server übertragen.

**DHCP\_RANGE\_x\_NTP\_SERVERS** legt die Adressen der NTP-Server fest.

Mehrere NTP-Server können durch Leerzeichen getrennt angegeben werden. Diese Variable ist optional. Wird hier nichts eingetragen, oder die Variable einfach weggelassen, wird die Einstellung aus [DHCP\\_NTP\\_SERVERS](#) verwendet. Es ist auch möglich, diese Variable auf 'none' zu setzen. Dann wird kein NTP-Server übertragen.

**DHCP\_RANGE\_x\_GATEWAY** legt die Adresse des Gateways für diese Range fest. Diese Variable ist optional. Wird hier nichts eingetragen, oder die Variable einfach weggelassen, wird die IP-Adresse des in DHCP\_RANGE\_x\_NET referenzierten Netzes verwendet. Es ist auch möglich, diese Variable auf 'none' zu setzen. Dann wird kein Gateway übertragen.

**DHCP\_RANGE\_x\_MTU** legt die MTU für Clients in diesem Range fest. Diese Variable ist optional.

**DHCP\_RANGE\_x\_OPTION\_WPAD** aktiviert oder deaktiviert die Übermittlung der DHCP-OPTION 252 (Web Proxy Autodiscovery Protocol) für diese DHCP-Range womit Browser automatisiert die Proxy-Einstellungen beziehen können. (siehe [http://de.wikipedia.org/wiki/Web\\_Proxy\\_Autodiscovery\\_Protocol](http://de.wikipedia.org/wiki/Web_Proxy_Autodiscovery_Protocol)) Diese Variable ist optional.

**DHCP\_RANGE\_x\_OPTION\_WPAD\_URL** definiert die URL der wpad.dat Datei oder wird leer gelassen um eine leere Antwort an den anfragenden Browser zu schicken, wodurch dieser keine weiteren regelmäßigen Anfragen durchführt. Diese Variable ist optional.

**DHCP\_RANGE\_x\_OPTION\_N** gestattet die Angabe Nutzer-definierter Optionen für diesen Bereich. Die verfügbaren Optionen kann man dem Manual des dnsmasq entnehmen (<http://thekelleys.org.uk/dnsmasq/docs/dnsmasq.conf.example>). Sie werden ungeprüft übernommen, können also bei Fehlern zu Problemen mit dem DNS/DHCP-Server führen. Diese Variable ist optional.

#### Extra DHCP-Range

**DHCP\_EXTRA\_RANGE\_N** legt die Anzahl von DHCP-Bereichen fest, die an nicht lokale Netze vergeben werden. Hierzu ist am Gateway zum entsprechenden Netz ein DHCP-Relay zu installieren.

**DHCP\_EXTRA\_RANGE\_x\_START** erste zu vergebende IP-Adresse.

**DHCP\_EXTRA\_RANGE\_x\_END** letzte zu vergebende IP-Adresse.

**DHCP\_EXTRA\_RANGE\_x\_NETMASK** Netzwerkmaske für diesen Bereich.

**DHCP\_EXTRA\_RANGE\_x\_DNS\_SERVERS** Adressen der DNS-Server  
(siehe [DHCP\\_RANGE\\_x\\_DNS\\_SERVERS](#)).

**DHCP\_EXTRA\_RANGE\_x\_WINS\_SERVERS** Adressen der WINS-Server  
(siehe [DHCP\\_RANGE\\_x\\_WINS\\_SERVERS](#)).

**DHCP\_EXTRA\_RANGE\_x\_NTP\_SERVERS** Adressen der NTP-Server  
(siehe [DHCP\\_RANGE\\_x\\_NTP\\_SERVERS](#)).

**DHCP\_EXTRA\_RANGE\_x\_GATEWAY** Adresse des Default-Gateway für diesen Bereich.

**DHCP\_EXTRA\_RANGE\_x\_MTU** legt die MTU für Clients in dieser Range fest. Diese Variable ist optional.

**DHCP\_EXTRA\_RANGE\_x\_DEVICE** Netzwerkinterface über den dieser Bereich erreicht wird.

#### Nicht zugelassene DHCP-Clients

**DHCP\_DENY\_MAC\_N** Anzahl der MAC-Adressen von Host, denen der Zugriff auf DHCP-Adressen verweigert wird.

**DHCP\_DENY\_MAC\_x** MAC-Adresse des Hosts, dem der Zugriff auf DHCP-Adressen verweigert wird.

### Unterstützung fürs Booten vom Netz

Der dnsmasq unterstützt Clients, die via Bootp/PXE übers Netz booten. Die dafür nötigen Informationen werden vom dnsmasq bereitgestellt und pro Subnetz und Host konfiguriert. Die dafür nötigen Variablen sind in den DHCP\_RANGE\_%- und HOST\_%-Abschnitten untergebracht und beschreiben das zu bootende File (\*\_PXE\_FILENAME), den Server, der dieses File bereitstellt (\*\_PXE\_SERVERNAME und \*\_PXE\_SERVERIP) und evtl. notwendige Optionen (\*\_PXE\_OPTIONS). Weiterhin kann man den internen tftp-Server aktivieren, so dass das Booten komplett von dnsmasq unterstützt wird.

**HOST\_x\_PXE\_FILENAME DHCP\_RANGE\_x\_PXE\_FILENAME** Hier wird das zu bootende Image angegeben. Im Falle von PXE wird hier der zu ladende pxe-Bootloader, wie z.B. pxegrub, pxelinux oder ein anderer passender Bootloader angegeben.

**HOST\_x\_PXE\_SERVERNAME HOST\_x\_PXE\_SERVERIP DHCP\_RANGE\_x\_PXE\_SERVERNAME** Name und IP des tftp-Servers, werden diese Variablen leer gelassen, wird der Router selbst als tftp-Server übermittelt.

**DHCP\_RANGE\_x\_PXE\_OPTIONS HOST\_x\_PXE\_OPTIONS** Einige Bootloader benötigen spezielle Optionen zum Booten. So erfragt zum Beispiel pxegrub über die Option 150 den Namen der Menu-Datei. Diese Optionen können hier angegeben werden und werden dann ins Konfigfile übernommen. Im Falle von pxegrub könnte das z.B. wie folgt aussehen:

```
HOST_x_PXE_OPTIONS='150,"(nd)/grub-menu.lst"'
```

Sind mehrere Optionen nötig, werden sie einfach mit Leerzeichen voneinander getrennt angegeben.

#### 4.6.4. DHCP-Relay

Das DHCP-Relay wird dann verwendet, wenn ein anderer DHCP-Server die Verwaltung der Ranges übernimmt, der nicht direkt von den Clients erreicht werden kann.

**OPT\_DHCPRELAY** Dieser Wert ist auf 'yes' zu setzen, damit der Router als DHCP-Relay arbeitet. Es darf nicht gleichzeitig ein DHCP-Server aktiv sein.

Standard-Einstellung: OPT\_DHCPRELAY='no'

**DHCPRELAY\_SERVER** An dieser Stelle wird der richtige DHCP-Server eingetragen, an den die Anfragen weitergereicht werden sollen.

**DHCPRELAY\_IF\_N DHCPRELAY\_IF\_x** Mit DHCPRELAY\_IF\_N gibt man die Anzahl der Netzwerkkarten an, auf denen der Relay-Server lauschen soll. In DHCPRELAY\_IF\_x werden dann die entsprechenden Netzwerkkarten angegeben.

Das Interface, über das die Antworten des DHCP-Servers wieder reinkommen, muß in der Liste mit aufgeführt werden. Zusätzlich muss sichergestellt werden, dass die Routen auf dem Rechner, auf dem der DHCP-Server läuft, korrekt gesetzt sind. Die Antwort des DHCP-Servers geht an die IP des Interfaces, an dem der DHCP-Client hängt. Nehmen wir folgendes Szenario an:

- Relay mit zwei Interfaces
- Interfaces zum Client: eth0, 192.168.6.1
- Interfaces zum DHCP-Server: eth1, 192.168.7.1
- DHCP-Server: 192.168.7.2

Dann muss es auf dem DHCP-Server eine Route geben, über den die Antworten an die 192.168.6.1 ihr Ziel erreichen. Ist der Router, auf dem das Relay läuft, der default gateway für den DHCP-Server, ist bereits alles ok. Ist dem nicht so, wird eine extra Route benötigt. Ist der DHCP-Server ein fli4l-Router, würde folgender Konfig-Eintrag dieses Ziel erreichen: `IP_ROUTE_x='192.168.6.0/24 192.168.7.1'`

Im Betrieb kann es zu Warnungen kommen, dass bestimmte Pakete ignoriert werden. Diese Warnungen kann man ignorieren, sie stören nicht den normalen Betrieb.

Beispiel:

```
OPT_DHCPRELAY='yes'
DHCPRELAY_SERVER='192.168.7.2'
DHCPRELAY_IF_N='2'
DHCPRELAY_IF_1='eth0'
DHCPRELAY_IF_2='eth1'
```

#### 4.6.5. DHCP-Client

Ein DHCP-Client kann verwendet werden, um eine IP-Adresse für eine oder mehrere Schnittstellen des Routers zu beziehen – dies erfolgt meist vom Service-Provider. Diese Möglichkeit der Anbindung kommt derzeit hauptsächlich bei Kabelmodem-Betreibern und in der Schweiz, in den Niederlanden und in Frankreich vor. Manchmal wird diese Konfiguration auch benötigt, wenn der Router hinter einem anderen Router eingebunden wird, der die Adressen per DHCP verteilt (z. B. FritzBox).

Die Konfiguration eines Netzwerks für DHCP erfordert zwei verschiedene Aktionen:

- Zum einen muss ein DHCP-Circuit konfiguriert werden, der DHCP für eine Schnittstelle aktiviert (s. u.).
- Zum anderen muss ein Netz via `IP_NET_x` definiert sein, dessen Schnittstelle mit der Circuit-Schnittstelle übereinstimmt und das auf den Namen des DHCP-Circuits gesetzt wird (siehe Beispiele weiter unten). Dadurch wird erst die Verbindung zwischen Netzwerk und DHCP-Circuit hergestellt.

Die Konfiguration der Netzwerk-Schnittstelle via DHCP wird immer dann durchgeführt, wenn der betreffende Circuit online geht; analog wird die erhaltene Adresse wieder freigegeben, wenn der Circuit offline geht. Routen werden gemäß der Variablen `CIRC_%_NETS_IPV4` gesetzt.

Das Paket wird über die Variable `OPT_DHCP_CLIENT` aktiviert:

**OPT\_DHCP\_CLIENT** Diese Variable muss auf 'yes' gesetzt werden, um DHCP-Circuits anlegen zu können.

Standard-Einstellung: `OPT_DHCP_CLIENT='no'`

#### 4. Pakete

Soll für ein Netz DHCP verwendet werden, so muss ein passender Circuit konfiguriert werden, siehe Abschnitt [Circuit-Konfiguration](#) (Seite 86). Der zu verwendende Typ in `CIRC_x_TYPE` lautet "dhcp". Zu den allgemeinen Circuit-Variablen kommen die folgenden hinzu, die DHCP-spezifisch sind:

**CIRC\_x\_DHCP\_DEV** In dieser Variable ist die Netzwerk-Schnittstelle vermerkt, für die das DHCP-Protokoll genutzt werden soll. Es ist sinnvoll, auf die Schnittstelle mit Hilfe der zugehörigen `IP_NET_x_DEV`-Variable zu verweisen.

Beispiel: `CIRC_1_DHCP_DEV='IP_NET_1_DEV'`

**CIRC\_x\_DHCP\_DAEMON** Das Paket kommt momentan mit zwei verschiedenen Implementierungen eines DHCP-Clients, `dhcpcd` und `dibbler`. Momentan wird `dhcpcd` nur für DHCPv4 und `dibbler` nur für DHCPv6 verwendet, so dass man nicht wirklich eine Wahl hat und diese Einstellung im besten Falle einfach nicht setzen sollte. Sollten später weitere Implementierungen unterstützt werden, wird die Auswahl über diese Variable erfolgen.

Beispiel 1: `CIRC_1_DHCP_DAEMON='dhcpcd'` Beispiel 2: `CIRC_1_DHCP_DAEMON='dibbler'`

Falls IPv6-Unterstützung aktiviert ist, muss darauf geachtet werden, dass nur IPv6-Netze (via `CIRC_x_NET_IPV6`) geroutet werden und die Variable `CIRC_x_NET_IPV4` nicht vorhanden oder leer ist. Auch ist zu beachten, dass der DHCPv6-Server in der Regel nicht eine einzelne Adresse, sondern ein ganzes IPv6-Subnetzpräfix zuweist (Prefix Delegation), so dass die `IPV6_NET_x`-Variable ein Suffix enthalten sollte (siehe hierzu die letzten beiden Beispiele weiter unten).

Es ist *nicht* möglich, mit Hilfe eines einzigen Circuits sowohl IPv4- als auch IPv6-Adressen via DHCP zu empfangen, Hierzu müssen zwei separate DHCP-Circuits eingerichtet werden.

Standard-Einstellung:

`CIRC_1_DHCP_DAEMON='dhcpcd'` (für IPv4)

`CIRC_1_DHCP_DAEMON='dibbler'` (für IPv6)

**CIRC\_x\_DHCP\_HOSTNAME** Manche Provider verlangen die Übermittlung eines Hostnamens. Dieser Name ist vom Provider zu erfahren und hier anzugeben. Er muss nicht zwangsläufig mit dem Hostnamen des Routers übereinstimmen.

Beispiel: `CIRC_1_DHCP_HOSTNAME='gandalf'`

Fehlt diese Variable oder ist sie leer, wird kein Hostname zum DHCP-Server gesandt.

Standard-Einstellung: `CIRC_1_DHCP_HOSTNAME=''`

**CIRC\_x\_DHCP\_STARTDELAY** Mit dieser Variable kann optional der Start des DHCP-Clients verzögert werden.

In manchen Installationen (z. B. fli4l als DHCP-Client hinter einem Kabelmodem oder einer FritzBox) ist es notwendig zu warten, bis der genutzte DHCP-Server z. B. nach einen Stromausfall ebenfalls neu gestartet worden ist.

Falls `CIRC_x_WAIT` ebenfalls verwendet wird, muss darauf geachtet werden, dass die Variable `CIRC_x_WAIT` größer als `CIRC_x_DHCP_STARTDELAY` ist, da ansonsten immer zu wenig Zeit zum Warten zur Verfügung steht.



Beispiel: `CIRC_1_DHCP_STARTDELAY='20'`

Standard-Einstellung: `CIRC_1_DHCP_STARTDELAY='0'`

**CIRC\_x\_DHCP\_ACCEPT\_CSR** Diese Variable steuert die Übernahme von zusätzlichen Routen, die der DHCP-Server senden kann. Für gewöhnlich wird dem DHCP-Client vom DHCP-Server nur ein Default-Router mitgeteilt. Gelegentlich passiert es jedoch, dass der DHCP-Server gar keinen Default-Router mitteilt und/oder andere Routen übermittelt. Das ist beispielsweise bei einem Telekom-Entertain-IPTV-Anschluss der Fall. In diesem Fall werden diese zusätzlichen Routen ebenfalls auf dem fli4l-Router installiert.

Diese Verarbeitung ist standardmäßig aktiviert. Vertrauen Sie Ihrem DHCP-Server jedoch nicht, können Sie die Verarbeitung der zusätzlichen Routen deaktivieren. Bedenken Sie jedoch, dass dann die korrekte Routing-Funktionalität nicht garantiert werden kann.

Beispiel: `CIRC_1_DHCP_ACCEPT_CSR='no'`

Standard-Einstellung: `CIRC_1_DHCP_ACCEPT_CSR='yes'`

Neben einem oder mehreren passenden Circuits müssen weiterhin ein oder mehrere passende Netze via `IP_NET_x` in der `config/base.txt` für den DHCP-Betrieb vorbereitet werden. Dazu müssen diese Variablen auf den Namen des jeweils zu verwendenden DHCP-Circuits oder eines seiner Schlagwörter (beides jeweils in geschweiften Klammern) gesetzt werden.

Beispiel 1 (IPv4):

```
IP_NET_N='1'
IP_NET_1='{circ1}' # alternativ '{dhcp0}'
IP_NET_1_DEV='eth1'
[...]
#
CIRC_N='1'
#
CIRC_1_NAME='DHCP-LAN'
CIRC_1_TYPE='dhcp'
CIRC_1_ENABLED='yes'
CIRC_1_NETS_IPV4_N='1'
CIRC_1_NETS_IPV4_1='0.0.0.0/0'
CIRC_1_UP='yes'
CIRC_1_WAIT='15'
CIRC_1_DHCP_DEV='IP_NET_1_DEV'
```

Beispiel 2 (IPv4 mit Nutzung von Schlagwörtern):

```
IP_NET_N='1'
IP_NET_1='{dhcp-lan}'
IP_NET_1_DEV='eth1'
[...]
#
CIRC_N='1'
#
CIRC_1_NAME='DHCP-LAN'
CIRC_1_TYPE='dhcp'
CIRC_1_ENABLED='yes'
```

#### 4. Pakete

```
CIRC_1_NETS_IPV4_N='1'  
CIRC_1_NETS_IPV4_1='0.0.0.0/0'  
CIRC_1_UP='yes'  
CIRC_1_WAIT='15'  
CIRC_1_DHCP_DEV='IP_NET_1_DEV'
```

Beispiel 3 (IPv6 mit DHCPv6-Server im LAN und Referenz über den Circuit-Namen):

```
IPV6_NET_N='1'  
IPV6_NET_1='{DHCPv6-LAN}::1:0:0:0:1/64'  
IPV6_NET_1_DEV='eth1'  
[...]  
#  
CIRC_N='1'  
#  
CIRC_1_NAME='DHCPv6-LAN'  
CIRC_1_TYPE='dhcp'  
CIRC_1_ENABLED='yes'  
CIRC_1_UP='yes'  
CIRC_1_WAIT='15'  
CIRC_1_DHCP_DEV='IPV6_NET_1_DEV'  
CIRC_1_PROTOCOLS='ipv6'
```

Beispiel 4 (IPv6 mit DHCPv6-Server auf der anderen Seite einer PPP-Verbindung):

```
IPV6_NET_N='1'  
IPV6_NET_1='{DHCPv6-manitu}::1:0:0:0:1/64'  
IPV6_NET_1_DEV='eth1'  
[...]  
#  
CIRC_N='2'  
#  
CIRC_1_NAME='DHCPv6-manitu'  
CIRC_1_TYPE='dhcp'  
CIRC_1_ENABLED='yes'  
CIRC_1_UP='yes'  
CIRC_1_WAIT='15'  
CIRC_1_DHCP_DEV='{DSL-manitu}'  
CIRC_1_PROTOCOLS='ipv6'  
#  
CIRC_2_NAME='DSL-manitu'  
CIRC_2_TYPE='ppp'  
CIRC_2_ENABLED='yes'  
CIRC_2_PPP_TYPE='ethernet'  
CIRC_2_NETS_IPV6_N='1'  
CIRC_2_NETS_IPV6_1='::/0'  
[...]
```

In den IPv4-Beispielen wird die Default-Route über den DHCP-Circuit gelegt. Ist das nicht erwünscht, muss `CIRC_x_NETS_IPV4_%` entsprechend geändert werden. Auch werden alle Circuits bereits beim Booten aktiviert (`CIRC_x_UP='yes'`), und der Boot-Vorgang wartet maximal 15 Sekunden darauf, dass der Router eine IP-Adresse erfolgreich via DHCP erhalten hat. Das

ist vor allem dann nötig, wenn andere Pakete eine vorhandene Netzanbindung während des Boot-Vorgangs erfordern.

In den IPv6-Beispielen werden *keine* Default-Routen über den DHCP-Circuit gelegt. Das liegt daran, dass bei DHCPv6 (im Gegensatz zum IPv4-Pendant) keine Informationen zum Routing versandt werden. Informationen über Next-Hop-Router werden hier über so genannte "Router Advertisements" verschickt.

### 4.6.6. TFTP-Server

Der TFTP-Server wird dann verwendet, wenn der fli4l per TFTP Dateien ausliefern soll. Dies kann zum Beispiel dazu dienen, das ein Client per Netboot startet.

**OPT\_TFTP** Aktiviert den internen TFTP-Server des dnsmasq. Standard-Wert ist 'no'.

**TFTP\_PATH** Spezifiziert das Verzeichnis, in dem die Dateien liegen, die der tftp-Server an die Klienten ausliefern soll. Die entsprechenden Dateien sind mit Hilfe eines geeigneten Programms (z.B. scp) im entsprechenden Pfad abzulegen.

### 4.6.7. YADIFA - Slave DNS Server

**OPT\_YADIFA** Aktiviert den YADIFA Slave DNS Server. Standard-Wert ist 'no'.

**OPT\_YADIFA\_USE\_DNSMASQ\_ZONE\_DELEGATION** Wenn diese Einstellung aktiviert wird erzeugt das yadifa Startscript automatisch für alle Slavezonen entsprechende Zone Delegation Einträge für den dnsmasq. Damit sind die Slavezonen auch direkt über den dnsmasq abfragbar und man benötigt im Prinzip keine YADIFA\_LISTEN\_x Einträge mehr. Die Anfragen werden dann vom dnsmasq beantwortet und einen nur auf localhost:35353 horchenden yadifa weitergeleitet.

**YADIFA\_LISTEN\_N** Wenn Sie OPT\_YADIFA='yes' gewählt haben, können Sie mit Hilfe von YADIFA\_LISTEN\_N die Anzahl, und mit YADIFA\_LISTEN\_1 bis YADIFA\_LISTEN\_N lokale IPs angeben, auf denen YADIFA DNS-Anfragen annehmen darf. Eine Portnummer ist optional möglich, mit der Angabe 192.168.1.1:5353 würde der YADIFA Slave DNS Server auf DNS Anfragen auf Port 5353 horchen. Achten Sie darauf, dass der dnsmasq in diesem Fall nicht auf allen Schnittstellen horchen darf (siehe DNS\_BIND\_INTERFACES). An dieser Stelle dürfen nur IPs von existierenden Schnittstellen (ethernet, wlan ...) verwendet werden, es kommt sonst zu Warnmeldungen beim Start des Routers. Alternativ ist nun möglich hier auch ALIAS-Namen zu verwenden, z. B. IP\_NET\_1\_IPADDR

### YADIFA\_ALLOW\_QUERY\_N

**YADIFA\_ALLOW\_QUERY\_x** Gibt IP-Adressen und Netze an denen der Zugriff auf YADIFA erlaubt ist. YADIFA nutzt die Angaben um den fli4l Paketfilter entsprechend zu konfigurieren und die Konfigurationsdateien von YADIFA zu erstellen. Mit dem Prefix ! wird der IP-Adresse oder dem Netz der Zugriff auf YADIFA verweigert.

Der fli4l Paketfilter wird für YADIFA so konfiguriert, dass alle erlaubten Netze aus dieser Einstellung und der für die einzelnen Zonen zusammen in eine ipset Liste (yadifa-allow-query) aufgenommen werden. Eine Unterscheidung nach Zonen ist beim Paketfilter leider

nicht möglich. Zusätzlich werden alle IP-Adressen und Netze aus dieser globalen Einstellung, denen der Zugriff verweigert wird, in diese Liste aufgenommen. Es ist daher nicht möglich den Zugriff später für einzelne Zonen wieder auszuweiten.

**YADIFA\_SLAVE\_ZONE\_N** Gibt die Anzahl der Slave DNS Zonen an die YADIFA verwalten soll.

**YADIFA\_SLAVE\_ZONE\_x** Der Name der Slave DNS Zone.

**OPT\_YADIFA\_SLAVE\_ZONE\_USE\_DNSMASQ\_ZONE\_DELEGATION** Aktiviert (=‘yes’) oder deaktiviert (=‘no’) die dnsmasq Zone Delegation nur für die Slavezone.

**YADIFA\_SLAVE\_ZONE\_x\_MASTER** Die IP-Adresse mit einer optionalen Portnummer des DNS Master Server.

**YADIFA\_SLAVE\_ZONE\_x\_ALLOW\_QUERY\_N**

**YADIFA\_SLAVE\_ZONE\_x\_ALLOW\_QUERY\_x** Gibt IP-Adressen und Netze an denen der Zugriff auf diese YADIFA DNS Zone erlaubt ist. Damit kann der Zugriff auf bestimmte DNS Zonen weiter eingeschränkt werden. YADIFA nutzt die Angaben um die Konfigurationsdateien von YADIFA zu erstellen.

Mit dem Prefix ! wird die IP-Adresse oder das Netz der Zugriff auf YADIFA verweigert.

## 4.7. DSLMODEM - PPP über internes DSL-Modem

Dieses Paket erlaubt es, PPP-Verbindungen über ein internes DSL-Modem wie den AVM Fritz!DSL-Adapter aufzubauen. Dieses interne DSL-Modem wird dabei direkt an den jeweiligen Netzzugang (in Deutschland an den Splitter) angeschlossen. Technisch “verpackt” das DSL-Modem die Pakete je nach Provider in PPPoE- oder PPPoA-Pakete; dies ist jedoch für den fli4l transparent. Hat man ein solches DSL-Modem, kann mit diesem Paket somit eine DSL-Verbindung ins Internet realisiert werden.

Ein solcher DSL-Zugang wird generell als PPP-Circuit konfiguriert (siehe [Circuits vom Typ “ppp”](#) (Seite 225)), d. h. es gilt:

```
CIRC_x_TYPE='ppp'
```

Zusätzlich muss das OPT\_PPP\_DSLMODEM aktiviert werden:

**OPT\_PPP\_DSLMODEM** Diese Variable aktiviert die Unterstützung für PPP über ein internes DSL-Modem. Damit auch tatsächlich eine solche Verbindung genutzt werden kann, muss mindestens ein PPP-Circuit den Typ “dslmodem” besitzen, d. h. es muss zusätzlich gelten

```
CIRC_x_TYPE='ppp'
CIRC_x_PPP_TYPE='dslmodem'
```

(wobei “x” einen gültigen Circuit-Index darstellt).

Standard-Einstellung: OPT\_PPP\_DSLMODEM='no'

Beispiel: OPT\_PPP\_DSLMODEM='yes'

**Wichtig:** Da die entsprechenden Treiber nicht der GPL unterliegen, müssen hierfür die nonfree-Varianten des gewünschten Kernel-Pakets verwendet werden.

Zu den allgemeinen Circuit-Variablen kommen die folgenden, für PPP/dslmodem-Circuits spezifischen Variablen hinzu:

**CIRC\_x\_PPP\_DSLSMODEM\_TYPE** Es gibt verschiedene interne DSL-Modems, über die eine DSL-Anbindung erfolgen kann. Das verwendete DSL-Modem wird mit Hilfe der Variablen CIRC\_x\_PPP\_DSLSMODEM\_TYPE eingestellt, wobei die in Tabelle 4.4 aufgeführten Typen zur Verfügung stehen.

Kartentyp	Internes DSL-Modem
fcdsl	AVM Fritz!Card DSL
fcdsl2	AVM Fritz!Card DSLv2
fcdslusb	AVM Fritz!Card DSL USB
fcdslusb2	AVM Fritz!Card DSL USBv2
fcdslsl	AVM Fritz!Card DSL SL
fcdslslusb	AVM Fritz!Card DSL SL USB

Tabelle 4.4.: Unterstützte interne DSL-Modems

Beispiel: CIRC\_x\_PPP\_DSLSMODEM\_TYPE='fcdsl'

**CIRC\_x\_PPP\_DSLSMODEM\_PROVIDER** Mit dieser Option wird der Typ der Gegenstelle eingestellt. Mögliche Optionen sind U-R2, ECI, Siemens, Netcologne, oldArcor, Switzerland, Belgium, Austria1, Austria2, Austria3 und Austria4. In Deutschland handelt es sich fast immer um UR-2. Siemens und ECI kommen nur bei sehr alten Anschlüssen zum Einsatz. Für Schweiz und Belgien sollten die Optionen selbsterklärend sein, und in Österreich heißt es ausprobieren.

Sollte jemand für Österreich eine bessere Beschriftung der Optionen haben, möge er diese bitte mitteilen.

Beispiel: CIRC\_x\_PPP\_DSLSMODEM\_PROVIDER='U-R2'

Beispiel (Internet-Zugang über DSL):

```
OPT_PPP='yes'
OPT_PPP_DSLSMODEM='yes'
#
CIRC_N='1'
CIRC_1_NAME='DSL-Manitu'
CIRC_1_TYPE='ppp'
CIRC_1_ENABLED='yes'
CIRC_1_NETS_IPV6_N='1'
CIRC_1_NETS_IPV6_1='::/0'
CIRC_1_CLASS_N='1'
CIRC_1_CLASS_1='internet'
CIRC_1_UP='yes'
CIRC_1_TIMES='Mo-Su:00-24:0.0:Y'
CIRC_1_USEPEERDNS='yes'
CIRC_1_PPP_TYPE='dslmodem'
```

```

CIRC_1_PPP_USERID='anonymer'
CIRC_1_PPP_PASSWORD='surfer'
CIRC_1_PPP_DSLMODEM_TYPE='fcdsl'
CIRC_1_PPP_DSLMODEM_PROVIDER='U-R2'
#
CIRC_CLASS_N='1'
CIRC_CLASS_1='internet'

```

## 4.8. DYNDNS - Dynamische Updates für Domain Name Services

Dieses Paket ist dafür gedacht, automatisch bei jeder Einwahl einen dynamischen Hostname zu aktualisieren. Folgende Dienste werden unterstützt:

Anbieter	FreeDNS (afraid.org)
DYNDNS_x_PROVIDER	AFRAID
Homepage	<a href="http://freedns.afraid.org">http://freedns.afraid.org</a>

**Wichtig:** Als Passwort ist hier der letzte Teil (hinter dem Fragezeichen) der URL anzugeben, die man auf der Homepage von Afraid.org abrufen kann (Einloggen ⇒ „Dynamic DNS“ ⇒ Die URL, die sich hinter dem Link „Direct URL“ versteckt). Alle anderen Angaben werden ignoriert.

Anbieter	Companity
DYNDNS_x_PROVIDER	COMPANITY
Homepage	<a href="http://www.staticip.de/">http://www.staticip.de/</a>

Anbieter	DDNSS
DYNDNS_x_PROVIDER	DDNSS
Homepage	<a href="http://www.ddnss.de/">http://www.ddnss.de/</a>

Anbieter	DHS International
DYNDNS_x_PROVIDER	DHS
Homepage	<a href="http://www.dhs.org/">http://www.dhs.org/</a>

Anbieter	DNS2Go
DYNDNS_x_PROVIDER	DNS2GO
Homepage	<a href="http://dns2go.com/">http://dns2go.com/</a>

Anbieter	DNS-O-Matic
DYNDNS_x_PROVIDER	DNSOMATIC
Homepage	<a href="http://www.dnsomatic.com">http://www.dnsomatic.com</a>

Anbieter	DtDNS
DYNDNS_x_PROVIDER	DTDNS
Homepage	<a href="http://www.dtdns.com/">http://www.dtdns.com/</a>

#### 4. Pakete

Anbieter	DynAccess
DYNDNS_x_PROVIDER	DYNACCESS
Homepage	<a href="http://dynaccess.de/">http://dynaccess.de/</a>

**Wichtig:** DynAccess bietet im Rahmen der fli4l-DynAccess-Kooperation für die Subdomains \*.dyn-fli4l.de, \*.dyn-fli4l.info und \*.dyn-eisfair.de Sondertarife an. Informationen hierzu gibt es auf der Internet-Seite <http://www.dyn-fli4l.de/> bzw. <http://www.dyn-eisfair.de/>.

Anbieter	DynDNS.org
DYNDNS_x_PROVIDER	DYNDNS
Homepage	<a href="http://dyn.com/">http://dyn.com/</a>

Anbieter	DynDNS.org (custom)
DYNDNS_x_PROVIDER	DYNDNSC
Homepage	<a href="http://dyn.com/standard-dns/">http://dyn.com/standard-dns/</a>

Anbieter	DynDNS DK
DYNDNS_x_PROVIDER	DYNDNSDK
Homepage	<a href="http://dyndns.dk/">http://dyndns.dk/</a>

Anbieter	dyndns:free
DYNDNS_x_PROVIDER	DYDNSFREE
Homepage	<a href="http://dyndnsfree.de/">http://dyndnsfree.de/</a>

Anbieter	eisfair.net
DYNDNS_x_PROVIDER	DYNEISFAIR
Homepage	<a href="http://www.intersales.de/it-infrastruktur/dyneisfair.html">http://www.intersales.de/it-infrastruktur/dyneisfair.html</a>

**Wichtig:** Mit der Benutzung dieses Dienstes unterstützt man die Arbeit der fli4l- und eisfair-Entwickler.

Anbieter	DyNS
DYNDNS_x_PROVIDER	DYNSCX
Homepage	<a href="http://www.dyns.cx/">http://www.dyns.cx/</a>

Anbieter	GnuDIP Dynamic DNS
DYNDNS_x_PROVIDER	GNUDIP
Homepage	<a href="http://gnudip2.sourceforge.net/">http://gnudip2.sourceforge.net/</a>

#### 4. Pakete

Anbieter	Provider Hurricane Electric
DYNDNS_x_PROVIDER	HE
Homepage	<a href="https://dns.he.net/">https://dns.he.net/</a>

Anbieter	IN-Berlin e.V.
DYNDNS_x_PROVIDER	INBERLIN
Homepage	<a href="http://www.in-berlin.de">http://www.in-berlin.de</a>

Anbieter	INWX GmbH	Co. KG
DYNDNS_x_PROVIDER	INWX	
Homepage	<a href="https://www.inwx.de/">https://www.inwx.de/</a>	

Anbieter	KONTENT
DYNDNS_x_PROVIDER	KONTENT
Homepage	<a href="http://www.kontent.de/">http://www.kontent.de/</a>

Anbieter	Nerdcamp.net
DYNDNS_x_PROVIDER	NERDCAMP
Homepage	<a href="http://nerdcamp.net/dynamic/dns.cgi">http://nerdcamp.net/dynamic/dns.cgi</a>

Anbieter	No-IP.com
DYNDNS_x_PROVIDER	NOIP
Homepage	<a href="http://www.no-ip.com/">http://www.no-ip.com/</a>

Anbieter	noxaDynDNS
DYNDNS_x_PROVIDER	NOXA
Homepage	<a href="http://www.noxa.de/">http://www.noxa.de/</a>

Anbieter	OVH.DE
DYNDNS_x_PROVIDER	OVHDE
Homepage	<a href="http://www.ovh.de/">http://www.ovh.de/</a>

Anbieter	PHPDYN
DYNDNS_x_PROVIDER	PHPDYN
Homepage	<a href="http://www.webnmail.de/phpdyn/">http://www.webnmail.de/phpdyn/</a>

**Wichtig:** diese Lösung muß man selber hosten

Anbieter	Regfish.com
DYNDNS_x_PROVIDER	REGFISH
Homepage	<a href="http://www.regfish.de/">http://www.regfish.de/</a>



#### 4. Pakete

Anbieter	SelfHost.de
DYNDNS_x_PROVIDER	SELFHOST
Homepage	<a href="http://selfhost.de/cgi-bin/selfhost">http://selfhost.de/cgi-bin/selfhost</a>

Anbieter	Securepoint Dynamic DNS Service
DYNDNS_x_PROVIDER	SPDNS
Homepage	<a href="http://www.spdns.de/">http://www.spdns.de/</a>

Anbieter	Strato
DYNDNS_x_PROVIDER	STRATO
Homepage	<a href="http://www.strato.de/">http://www.strato.de/</a>

Anbieter	T-Link.de
DYNDNS_x_PROVIDER	TLINK
Homepage	<a href="http://www.t-link.de/">http://www.t-link.de/</a>

Anbieter	twodns.de
DYNDNS_x_PROVIDER	TWODNS
Homepage	<a href="http://www.twodns.de/">http://www.twodns.de/</a>

Anbieter	ZoneEdit.com
DYNDNS_x_PROVIDER	ZONEEDIT
Homepage	<a href="http://zoneedit.com/">http://zoneedit.com/</a>

Wir versuchen diese Daten aktuell zu halten. Trotzdem übernehmen wir keine Haftung für die Richtigkeit dieser Daten. Wer einen Fehler oder eine Änderung entdeckt sollte eine Mail an das fli4l-Team (E-Mail: [team@fli4l.de](mailto:team@fli4l.de)) schicken.

Diese Liste ist komplett, andere Provider werden ohne Änderung nicht unterstützt. Wie man das Paket um eigene Anbieter erweitern kann, steht im Anhang.

Der dynamische Hostname wird automatisch bei jeder Einwahl ins Internet aktualisiert. Das Paket beinhaltet eine Sperre, die das mehrmalige aktualisieren der gleichen IP verhindert, da dies bei einigen DynDNS-Anbietern nicht gerne gesehen wird und im Extremfall zur Sperrung des Accounts führen kann.

Hinweis: Es kann einige Minuten dauern, bis die Änderung des dynamischen Hostnamens wirksam wird.

Bevor man mit der Einrichtung dieses Paketes beginnen kann, muss man sich bei einem der oben genannten Anbietern einen Account holen. Falls man das schon hat, kann man sofort loslegen. Hat man noch keinen Account, so kann man sich an obiger Tabelle orientieren, um einen Hostname zu finden, der den Ansprüchen genügt und den persönlichen Geschmack trifft.

Für die nun folgende Konfiguration benötigt man folgende Daten:

- Name des Anbieters
- Benutzername
- Passwort

- Den DynDNS-Hostnamen

Die benötigten Angaben können je nach Anbieter variieren, es wird versucht eine möglichst konsistente Konfiguration zu bieten. Manchmal ist z.B. der Hostname gleich dem Benutzernamen, in so einem Fall werden wir versuchen, immer das Host-Feld zu benutzen und den Benutzernamen einfach ignorieren. Jetzt aber los:

**OPT\_DYNDNS** Steht dieser Parameter auf 'yes', wird OPT\_DYNDNS aktiviert.

**DYNDNS\_SAVE\_OUTPUT** Wird dieser Parameter auf 'yes' gestellt, wird das Ergebnis der DynDNS-Anfrage(n) in einer Datei gespeichert und kann über den Webserver<sup>3</sup> abgefragt werden.

**DYNDNS\_N** Hat man bei mehreren DynDNS-Anbietern einen Account und will deswegen bei jeder Einwahl mehrere Namen updaten, so ist dieser Wert entsprechend anzupassen.

**DYNDNS\_x\_PROVIDER** Hier wird der Name des zu benutzenden Providers angegeben (siehe Tabelle weiter oben und Hinweis in der Config-Datei).

**DYNDNS\_x\_USER** Benutzername bei dem DynDNS-Anbieter. Häufig ist dies eine E-Mail-Adresse, ein selbstgewählter Name oder gleich dem DynDNS-Hostname.

**DYNDNS\_x\_PASSWORD** Hier ist das Passwort des DynDNS-Accounts anzugeben. Aufpassen, dass niemand anderes beim Editieren der Config-Datei zusieht!

**DYNDNS\_x\_HOSTNAME** Hier ist der *komplette* DynDNS-Hostname des Accounts einzutragen. Beispielsweise könnte hier folgendes stehen:

- cool.nerdcamp.net
- user.dyndns.org
- fli4luser.fli4l.net

**DYNDNS\_x\_UPDATEHOST** Hier wird für den Provider PHPDYN angegeben, auf welchem Host der Updater installiert ist. Dies ist nötig, da dies kein herkömmlicher Provider ist sondern nur ein Script, welches einen PowerDNS Server mit MySQL aktualisiert und welches unter der GPL steht.

**DYNDNS\_x\_CIRCUIT** Hier kann angegeben werden, bei welchen Circuits dieser Hostname aktualisiert wird. Die einzelnen Circuits werden mit Leerzeichen voneinander getrennt. Es kann z.B. erwünscht sein, den Hostnamen nur bei der DSL-Einwahl zu benutzen. Hier ein paar Beispiele:

```
DYNDNS_1_CIRCUIT='1 2 3'           # Nur ISDN: Circuits 1 bis 3
oder
DYNDNS_1_CIRCUIT='pppoe'           # Nur DSL: pppoe-Circuit
oder
DYNDNS_1_CIRCUIT='dhcp'            # Update bei DHCP-Providern
                                   # (opt_dhcp wird benötigt)
oder
DYNDNS_1_CIRCUIT='pppoe 1'         # DSL und ISDN
```

<sup>3</sup>OPT\_HTTPD im Paket HTTPD (Seite 165) auf <http://www.fli4l.de/download/stabile-version/>

**DYNDNS\_x\_RENEW** Manche Provider erwarten, dass alle *n* Tage ein Update ausgeführt wird, auch wenn sich die IP nicht verändert hat. Dieses Intervall kann man hier angeben. Gibt man keinen Wert an, wird nach 29 Tagen ein Update durchgeführt.

Zu beachten ist hierbei, dass ein Update nur bei einer Einwahl angestoßen wird - also bei einer Einwahl über DSL oder ISDN oder einer Erneuerung einer Lease bei einem via DHCP konfigurierten Interface, wie man es bei einem Kabelmodem findet. Findet über längere Zeit keine Einwahl statt, muß man das Update auf andere Weise anstoßen.

#### **DYNDNS\_x\_EXT\_IPV4**

**DYNDNS\_x\_EXT\_IPV6** Mit dieser Variable wird die Methode, mit der die externe IP Adresse ermittelt wird, konfiguriert. Im Moment gibt es die Möglichkeit mit **'none'** überhaupt keinen externen Dienst nach der IP Adresse zu befragen sondern direkt die externe IP Adresse anhand des WAN Interfaces zu bestimmen. Das funktioniert in der Regel aber nur bei WAN Verbindungen, die direkt auf dem fli4l terminieren, wie z.B. DSL via PPPoE. Mit der Einstellung **'dyndns'** wird die beim Update verwendete IP Adresse über den externen Dienst von checkip.dyndns.org ermittelt. Wird die Einstellung **'stun'** benutzt wird die Liste der STUN Server der Reihe nach abgefragt bis eine erfolgreiche Antwort geliefert wird. Die Nutzung eines externen Dienstes zur Ermittlung der IP Adresse ist notwendig, wenn der Router selbst nicht derjenige ist, der die externe IP erhält. Dabei ist zu beachten, dass der Router in diesem Falle momentan eine Änderung der externen IP nicht mitbekommt, den dyndns-Namenseintrag also nicht zeitnah aktualisieren kann.

**DYNDNS\_x\_LOGIN** Manche Provider erfordern, dass sich der Benutzer regelmäßig auf ihrer Internet-Seite unter seinem Benutzerkonto anmeldet, damit der Dienst nicht deaktiviert wird. Wenn diese Variable auf **'yes'** gesetzt ist, erledigt das der fli4l für Sie. Allerdings funktioniert das nur, wenn das dyndns-Paket für den jeweiligen Provider vorbereitet wurde. Momentan ist eine solche regelmäßige Anmeldung nur für den Provider "DYNDNS" erforderlich und möglich. Bedenken Sie bitte auch, dass die Nutzung dieser Funktion **OPT\_EASYCRON='yes'** im Paket easycron erfordert.

**DYNDNS\_LOGINTIME** Nutzen Sie einen Provider, bei dem sich der fli4l regelmäßig anmelden soll, um eine Deaktivierung des Dienstes zu verhindern (s.o.), dann können Sie mit dieser Variable einstellen, wann diese Anmeldung stattfinden soll. Benötigt wird eine Zeitangabe im Cron-Format; zu Details lesen Sie sich bitte die Dokumentation des easycron-Pakets durch. Die Standardbelegung lautet **0 8 \* \* \***, was einer täglichen Anmeldung um acht Uhr morgens entspricht.

**DYNDNS\_ALLOW\_SSL** Ist diese Variable auf **'yes'** gesetzt, wird das Update wenn möglich über SSL (verschlüsselte Verbindung) durchgeführt.

**DYNDNS\_LOOKUP\_NAMES** Ein Update der IP sollte eigentlich nur erfolgen, wenn sich die IP geändert hat. Viele fli4l-Router haben jedoch keinen permanenten Speicher, auf der die Information über die registrierte IP gesichert werden kann, daher steht diese Information direkt nach dem Booten dort nicht zur Verfügung. Um trotzdem unnötige Updates zu vermeiden, kann fli4l in dieser Situation (und nur in dieser Situation) beim Namensdienst nach der aktuell registrierten IP fragen. Die ermittelte IP wird dann zwischengespeichert und für jedes weitere Update genutzt.

Zu beachten ist dabei, dass nach einem Reboot das Update-Intervall neu beginnt, wenn fli4l den Namensdienst zur Ermittlung der IP nutzt.

**DYNDNS\_DEBUG\_PROVIDER** Ist diese Variable auf 'yes' gesetzt, wird ein trace des Update-Vorgangs aufgezeichnet, so dass man im Nachhinein bei einem Problem prüfen kann, was schief gegangen ist. Default: DYNDNS\_DEBUG\_PROVIDER='no'

**OPT\_STUN** Mit 'yes' wird die Funktionalität zur Ermittlung der externen IP-Adresse über STUN-Server aktiviert

**STUN\_SERVER\_N** Mit dieser Variable wird die Anzahl der STUN-Server definiert.

**STUN\_SERVER\_x** FQDN des STUN-Server, optional kann der FQDN um den zu verwendenden Port ergänzt werden

```
STUN_SERVER_1='stun.1.google.com:19302'  
STUN_SERVER_2='stun1.1.google.com:19302'  
STUN_SERVER_3='stun2.1.google.com:19302'  
STUN_SERVER_4='stun3.1.google.com:19302'  
STUN_SERVER_5='stun4.1.google.com:19302'  
STUN_SERVER_6='stun01.sipphone.com'  
STUN_SERVER_7='stun.ekiga.net'  
STUN_SERVER_8='stun.fwdnet.net'  
STUN_SERVER_9='stun.ideasip.com'
```

## 4.9. EASYCRON - Befehle zeitgesteuert ausführen

Dieses Paket wurde von Stefan Manske E-Mail: [fli4l@stephan.manske-net.de](mailto:fli4l@stephan.manske-net.de) zusammengestellt und vom fli4l-Team an 2.1 angepaßt.

### 4.9.1. Konfiguration

Mit OPT\_EASYCRON kann man über das entsprechende config-file gesteuert zu bestimmten Zeiten Befehle ausführen lassen.

Dabei werden folgende Einträge benutzt:

**OPT\_EASYCRON** mit OPT\_EASYCRON='yes' wird das Paket aktiviert

Standard-Einstellung: OPT\_EASYCRON='no'

**EASYCRON\_MAIL** Da immer wieder Probleme auftraten, dass der crond unerwünschte Mails verschickt, kann man dies generell mit diesem Flag verhindern.

Standard-Einstellung: EASYCRON\_MAIL='no'

**EASYCRON\_N** Die Anzahl der verschiedenen Befehle, die von cron gestartet werden sollen.

**EASYCRON\_x\_CUSTOM** Wer sich mit den Einstellungen in der crontab auskennt, kann hier für jeden Eintrag eigene Einstellungen wie MAILTO, PATH, ... einstellen. Mehrere Einträge müssen durch \ getrennt werden. Hier sollte man sich aber wirklich mit cron auskennen.

Standard-Einstellung: EASYCRON\_CUSTOM=""

**EASYCRON\_x\_COMMAND** In EASYCRON\_x\_COMMAND wird der gewünschte Befehl eingetragen, wie z.B.

```
EASYCRON_1_COMMAND='echo 1 '>' /dev/console'
```

**EASYCRON\_x\_TIME** In EASYCRON\_x\_TIME wird die Ausführungszeit gemäß der üblichen cron-Syntax eingetragen.

### 4.9.2. Beispiele

- Der Computer wünscht uns “Ein gutes neues Jahr”

```
EASYCRON_1_COMMAND = 'echo Ein gutes neues Jahr! > /dev/console'  
EASYCRON_1_TIME     = '0 0 31 12 *'
```

- xxx wird von Montag bis Freitag jeweils von 7-20 Uhr zu jeder vollen Stunde ausgeführt.

```
EASYCRON_1_COMMAND = 'xxx'  
EASYCRON_1_TIME     = '0 7-20 0 * 1-5'
```

- Der Router beendet jede Nacht um 03:40 die Internet-Verbindung die per DSL aufgebaut ist baut sie nach 5sec Wartezeit wieder auf. Die folgenden Devicenamen sind möglich: pppoe, ippp[1-9], ppp[1-9].

```
EASYCRON_1_COMMAND = 'fli4lctrl hangup pppoe; sleep 5; fli4lctrl dial pppoe'  
EASYCRON_1_TIME     = '40 3 * * *'
```

Weitere Informationen zur cron-Syntax finden Sie unter

- <http://www.pro-linux.de/artikel/2/146/der-batchdaemon-cron.html>
- [http://de.linwiki.org/wiki/Linuxfibel\\_-\\_System-Administration\\_-\\_Zeit\\_und\\_Steuerung#Die\\_Datei\\_crontab](http://de.linwiki.org/wiki/Linuxfibel_-_System-Administration_-_Zeit_und_Steuerung#Die_Datei_crontab)
- <http://web.archive.org/web/20021229004331/http://www.linux-magazin.de/Artikel/ausgabe/1998/08/Cron/cron.html>
- [http://web.archive.org/web/20070810063838/http://www.newbie-net.de/anleitung\\_cron.html](http://web.archive.org/web/20070810063838/http://www.newbie-net.de/anleitung_cron.html)

### 4.9.3. Voraussetzungen

- fli4l in einer Version > 2.1.0
- für ältere Versionen bitte die entsprechenden opt\_easycron-Versionen aus der OPT-Datenbank verwenden

### 4.9.4. Installation

OPT\_EASYCRON wird einfach wie jedes andere OPT im aktuelle fli4l-Verzeichnis entpackt.

## 4.10. HD - Unterstützung von Festplatten, Flash-Karten, USB-Sticks usw.

### 4.10.1. OPT\_HDINSTALL - Installation auf Festplatte/CompactFlash

fli4l unterstützt eine Vielzahl an Bootmedien (CD, HD, Netzwerk, Compact-Flash,...). Die Diskette zählt aus Platzgründen ab Version 4.0 nicht mehr dazu.

Im Folgenden werden die notwendigen Schritte zur Installation auf einer Festplatte erklärt.

Der übliche Weg ist die Installation mit einem Bootmedium, es kann aber auch über Netzwerk-Boot installiert werden. Das OPT\_HDINSTALL bereitet die Festplatte vor. Ist beim Erstellen des Bootmediums sowohl dort als auch beim Ziel der Installation der gewählte `BOOT_TYPE='hd'` werden die Installationsdateien direkt übertragen. Sollte ein direktes Kopieren nicht möglich sein werden diese später über scp oder über ein Remote-Update per Imonc übertragen.

Eine Einführung in die verschiedenen Festplatten- Installationsvarianten A oder B befindet sich am [Anfang der fli4l-Dokumentation](#) (Seite 15). Bitte unbedingt vorher lesen!

#### HD-Installation in sechs einfachen Schritten

1. lauffähiges fli4l-Bootmedium mit dem Paket base sowie OPT\_HDINSTALL erstellen. Zusätzlich muss dieses Bootmedium ein Remote-Update ermöglichen. Es muss also entweder OPT\_SSHD aktiv sein oder OPT\_IMOND auf 'yes' stehen. Wenn zum Ansprechen des Datenträgers Treiber erforderlich sind, die in der Standardinstallation nicht enthalten sind, müssen diese zusätzlich über OPT\_HDDRV aktiviert werden.
2. den Router mit diesem Bootmedium booten.
3. am Router einloggen und den Befehl "hdinstall.sh" ausführen.
4. wenn die Aufforderung dazu erscheint die Dateien syslinux.cfg, kernel, rootfs.img, opt.img und rc.cfg mittels scp oder Imonc auf den Router nach /boot kopieren. Es wird empfohlen, dazu mit zwei fli4l-Verzeichnissen zu arbeiten, eines für das Setup und ein zweites für die spätere HD-Version. Bei der HD-Version stellen Sie die Variable `BOOT_TYPE='hd'` ein und beim Bootmedium dessen Typ entsprechend.

**Beim Remote-Update müssen natürlich die Dateien der HD-Version auf den Router übertragen werden!**

5. Bootmedium entfernen, Router herunterfahren und neu starten (unter Verwendung von halt/reboot/poweroff). Der Router bootet jetzt von der Festplatte
6. bei Problemen den folgenden Abschnitt gut durchlesen.

#### HD-Installation ausführlich erklärt (inklusive Beispielen)

Zuerst muss ein Router-Bootmedium erstellt werden, bei dem in der Datei config/hd.txt das OPT\_HDINSTALL mit den Installationsskripten und eventuell das OPT\_HDDRV (falls zusätzliche Treiber benötigt werden) richtig konfiguriert wurden. Bitte dazu auch den Abschnitt zu OPT\_HDDRV gründlich durchlesen!

#### 4. Pakete

Die Variable `BOOT_TYPE` in der `base.txt` wird entsprechend dem gewählten Setup-Medium eingestellt, es soll ja schließlich ein Setup durchgeführt werden. Die Variable `MOUNT_BOOT` in der `base.txt` muss auf `'rw'` eingestellt werden, damit später ggf. neue Archive (\*.img) über das Netzwerk aufgespielt werden können.

Anschließend wird der Router von diesem Setup-Bootmedium gebootet. Durch Eingabe von `"hdinstall.sh"` an der `fl4l`-Console wird dann das Installationsprogramm gestartet. Nach Beantwortung von ein paar Fragen wird auf die Festplatte installiert. Eventuell erscheint am Ende noch die Aufforderung, dass man die für den Router benötigten Dateien per Remote-Update aufspielen soll.

**Dieses Remote-Update keinesfalls vergessen, der Router bootet sonst nicht von der Festplatte. Zum Neustarten des Routers nach dem Remote-Update unbedingt reboot/halt/poweroff verwenden, andernfalls können die beim Remote-Update vorgenommenen Änderungen verloren gehen.**

Das Installationsscript kann sowohl direkt am Router als auch über `ssh` von einem anderen PC aus gestartet werden. Im jedem Fall muss man sich vorher durch Eingabe des Passwortes am Router anmelden. Als `ssh`-Client für Windows-Rechner kann z.B. die Freeware Putty verwendet werden.

#### Konfiguration des Setup-Bootmediums

<code>BOOT_TYPE</code>	entsprechend dem Bootmedium für die Installation einstellen
<code>MOUNT_BOOT='rw'</code>	notwendig, um später neue Archive (*.img) über Netzwerk auf die Platte kopieren zu können
<code>OPT_HDINSTALL='yes'</code>	notwendig um das Setup-Skript und die Tools zum Formatieren der Partitionen auf dem Bootmedium zu haben
<code>(OPT_HDDRV='yes')</code>	nur dann notwendig, wenn ohne spezielle Treiber nicht auf die Festplatte zugegriffen werden kann
<code>OPT_SSHD='yes'</code>	nach dem Vorbereiten der Festplatte werden eventuell noch Dateien per remote Update übertragen. Dazu benötigt man entweder den <code>sshd</code> , <code>imond</code> ( <code>IMOND='yes'</code> ) oder ein anderes Paket, das einen Filetransfer erlaubt.

Tabelle 4.5.: Beispiel für die Konfiguration des Setup-Mediums

Bereits hier muss die Netzwerkkonfiguration richtig eingestellt sein damit man später noch Dateien über das Netzwerk aufspielen kann. Es wird empfohlen, `DNS_DHCP` zu diesem Zeitpunkt noch nicht zu aktivieren, da dies regelmäßig zu Problemen führt (der DHCP-Server hat vielleicht noch eine lease für den zu installierenden Router). Für ein Remote-Update mittels `scp` (befindet sich im Paket `SSHD`) bitte `OPT_SSHD='yes'` einstellen. Alternativ dazu kann man die Dateien per `IMOND` übertragen, dafür wird zusätzlich allerdings eine gültige DSL oder ISDN-Konfiguration benötigt. Alle nicht unbedingt nötigen Pakete bitte weglassen, also kein `DNS_DHCP`, `SAMBA_LPD`, `LCD`, `Portforwarding` usw.

Falls die Installation mit der Fehlermeldung

```
*** ERROR: can't create new partition table, see docu ***
```

abbricht, können mehrere Fehlerquellen in Frage kommen:

- die Festplatte ist in Benutzung, evtl. durch einen abgebrochenen Installationsversuch. Einfach neu booten und noch einmal versuchen.
- es werden zusätzliche Treiber benötigt, siehe `OPT_HDDRV`
- es gibt Hardwareprobleme, mehr dazu bitte im Anhang nachlesen.

Im letzten Schritt kann man nun die endgültige Fassung der Konfigurationsdateien erstellen und alle gewünschten Pakete hinzufügen.

### Beispiele für eine fertige Installation nach Typ A und Typ B:

Ein Beispiel für jede Konfiguration finden Sie in Tabelle 4.6.

<code>BOOT_TYPE='hd'</code>	notwendig, da sie ja jetzt von Festplatte starten
<code>MOUNT_BOOT='rw ro no'</code>	nach Wahl. Um später neue fli4l-Archive über Netzwerk auf die Platte kopieren zu können ist 'rw' nötig.
<code>OPT_HDINSTALL='no'</code>	nach der erfolgreichen Installation ist dieses Paket nicht mehr notwendig.
<code>OPT_MOUNT</code> ( <code>OPT_HDDRV='yes'</code> )	nur aktivieren, falls eine Datenpartition erstellt wurde nur notwendig, wenn ohne zusätzliche Treiber nicht auf die Festplatte zugegriffen werden kann.

Tabelle 4.6.: Beispiel für eine Installation nach Typ A oder B

Das Erstellen einer Swap-Partition wird nur angeboten, falls weniger als 32MB RAM im Router stecken und die Installation NICHT auf ein Flash-Medium durchgeführt wird!

#### 4.10.2. `OPT_MOUNT` - Automatisches Einhängen von Dateisystemen

`OPT_MOUNT` hängt eine bei der Installation erstellte Datenpartition nach `/data` ein, eine Prüfung der Partition auf Fehler wird bei Bedarf automatisch durchgeführt. Ein evtl. vorhandenes CD-ROM wird nach `/cdrom` eingehängt, falls eine CD eingelegt ist. Für die swap-Partition wird das `OPT_MOUNT` nicht mehr benötigt!

**`OPT_MOUNT` liest die Konfigurationsdatei `hd.cfg` auf der Boot-Partition und hängt die dort angegebenen Partitionen ein. Wenn das `OPT_MOUNT` mit einem Remote-Update auf einen bereits installierten Router übertragen wurde, muss diese Konfigurationsdatei ggf. geändert werden.**

**Auch bei einem Boot von CD-ROM kann das `OPT_MOUNT` nicht genutzt werden. Die CD kann in diesem Fall mit `MOUNT_BOOT='ro'` eingehängt werden.**

Die Datei `hd.cfg` auf der DOS-Partition hat für einen Router nach Typ B mit Swap und Datenpartition den folgenden Inhalt (Beispiel):

```
hd_boot='sda1'
hd_opt='sda2'
hd_swap='sda3'
```



```
hd_data='sda4'
hd_boot_uuid='4A32-0C15'
hd_opt_uuid='c1e2bfa4-3841-4d25-ae0d-f8e40a84534d'
hd_swap_uuid='5f75874c-a82a-6294-c695-d301c3902844'
hd_data_uuid='278a5d12-651b-41ad-a8e7-97ccbc00e38f'
```

Nicht existierende Partitionen werden einfach weggelassen, bei einem Router Typ A ohne weitere Partitionen sieht das also so aus:

```
hd_boot='sda1'
hd_boot_uuid='4863-65EF'
```

### 4.10.3. OPT\_EXTMOUNT - Manuelles Einhängen von Dateisystemen

OPT\_EXTMOUNT hängt Datenpartitionen an jedem beliebigen Mountpoint im Dateisystem ein. Damit ist es möglich von Hand erstellte Dateisysteme einzuhängen und beispielsweise für einen Rsync-Server zur Verfügung zu stellen.

**EXTMOUNT\_N** Die Anzahl der Datenpartitionen die extra eingehängt werden sollen.

**EXTMOUNT\_x\_VOLUMEID** Device, Label oder UUID des Volumens, das eingehängt werden soll. Mit dem Befehl 'blkid' kann man sich Device, Label und UUID aller verfügbaren Volumen anzeigen lassen.

**EXTMOUNT\_x\_FILESYSTEM** Das verwendete Dateisystem der Partition. fließt unterstützt zur Zeit die Dateisysteme isofs, fat, vfat, ext2, ext3 und ext4.  
(Der Standardwert EXTMOUNT\_x\_FILESYSTEM='auto' versucht das verwendete Dateisystem automatisch festzustellen.)

**EXTMOUNT\_x\_MOUNTPOINT** Der Pfad (Mountpoint) im Dateisystem in dem das Device eingehängt wird. Der Pfad muss vorher nicht existieren, er wird automatisch erzeugt.

**EXTMOUNT\_x\_OPTIONS** Wenn spezielle Optionen an den 'mount' Aufruf übergeben werden sollen können diese hier angegeben werden.

**EXTMOUNT\_x\_HOTPLUG** Wenn diese Variable den Wert 'yes' enthält, ist es kein Fehler, wenn zur Boot-Zeit die Datenpartition nicht existiert. In diesem Fall wird davon ausgegangen, dass der zugehörige Datenträger fehlt und ggf. später eingebunden wird (z.B. via SATA-Hotplugging oder als USB-Stick). Das Aktivieren dieser Option erfordert zwingend OPT\_AUTOMOUNT='yes'. Des Weiteren muss zur Identifikation der gewünschten Datenpartition die eindeutige Kennung (UUID) des Dateisystems in EXTMOUNT\_x\_VOLUMEID eingetragen werden; andere IDs wie Gerätenamen oder Label werden *nicht* unterstützt.

Beispiel:

```
EXTMOUNT_1_VOLUMEID='sda2'      # device
EXTMOUNT_1_FILESYSTEM='ext3'    # filesystem
EXTMOUNT_1_MOUNTPOINT='/mnt/data' # mountpoint for device
EXTMOUNT_1_OPTIONS=''          # extra mount options passed via mount -o
EXTMOUNT_1_HOTPLUG='no'        # device must exist at boot time
```

#### 4.10.4. OPT\_AUTOMOUNT – automatisches Einhängen von Datenpartitionen

OPT\_AUTOMOUNT='yes' erlaubt es, Datenpartitionen automatisch und dynamisch während der Laufzeit einzuhängen. Es gibt zwei Konfigurationsvarianten. Die erste arbeitet mit OPT\_EXTMOUNT zusammen und hängt nur Datenpartitionen ein, die beim Booten gefehlt haben. Die zweite ist unabhängig von OPT\_EXTMOUNT und hängt *alle* lesbaren Datenpartitionen ein, egal ob bereits während des Bootens oder erst später. Steuern lässt sich das Verhalten mit Hilfe der Variablen AUTOMOUNT\_UNKNOWN:

**AUTOMOUNT\_UNKNOWN** Diese Variable steuert, ob unbekannte Datenpartitionen eingehängt werden. Mit AUTOMOUNT\_UNKNOWN='no' werden nur Datenpartitionen dynamisch während der Laufzeit eingehängt, die einem EXTMOUNT\_x-Eintrag entsprechen. Dazu muss zusätzlich EXTMOUNT\_x\_HOTPLUG='yes' definiert sein, damit OPT\_EXTMOUNT nicht meckert, wenn die Datenpartition beim Booten fehlen sollte. Mit AUTOMOUNT\_UNKNOWN='yes' werden auch unbekannte Datenpartitionen eingehängt. Dies funktioniert aber nur, wenn das Dateisystem auf der Datenpartition eine eindeutige Kennung (UUID) besitzt. In diesem Fall wird die Datenpartition in dem Verzeichnis /media/<UUID> eingehängt (dieses Verzeichnis wird bei Bedarf erzeugt).

Standard-Einstellung: AUTOMOUNT\_UNKNOWN='no'

**AUTOMOUNT\_UNKNOWN\_OPTS** Diese Variable gibt die mount-Optionen an, die bei unbekannten Datenpartitionen beim Einhängen verwendet werden. Ist die Datenpartition über OPT\_EXTMOUNT in der /etc/fstab identifizierbar, dann werden die hier angegebenen Optionen *nicht* benutzt; vielmehr werden die Optionen im passenden EXTMOUNT\_x\_OPTIONS-Eintrag genutzt.

Standard-Einstellung: AUTOMOUNT\_UNKNOWN\_OPTS='ro' (damit werden Schreibzugriffe auf unbekannte Datenpartitionen standardmäßig verhindert)

Jede Datenpartition wird vor dem Einhängen mit Hilfe des für das jeweilige Dateisystem verfügbaren Prüfprogramms auf Fehler überprüft (e2fsck für ext2/ext3/ext4-Dateisysteme und fsck.fat für (V)FAT-Dateisysteme). Schlägt die Prüfung oder die automatische Korrektur fehl, wird das Dateisystem *nicht* eingehängt, um Datenkorruption zu vermeiden.

Wird ein Gerät entfernt, auf dem ein Dateisystem eingehängt war, wird dies nachträglich via umount ausgehängt. Natürlich können dabei womöglich noch nicht geschriebene Daten nicht mehr gesichert werden (schließlich ist der Datenträger nicht mehr da), aber immerhin kann nicht mehr versucht werden, auf den nicht mehr vorhandenen Datenträger weiter zuzugreifen. Die korrekte Vorgehensweise ist natürlich *erst* das Dateisystem auszuhängen und *dann* den Datenträger zu entfernen. Weil nicht alle Gerätetypen ein Entfernen verhindern, wenn das Dateisystem eingehängt ist (beispielsweise funktioniert dies gut bei CD-Laufwerken), muss man sich unter Umständen selbst um die korrekte Reihenfolge der+ Aktionen kümmern.

Alle Aktivitäten von OPT\_AUTOMOUNT werden in der Datei /var/log/automount.log protokolliert. Ein beispielhafter Ausschnitt einer solchen Log-Datei wird im Folgenden gezeigt. Zuerst kommt der Abschnitt, der die Aktivitäten für Datenpartitionen aufzeigt, die bereits während des Bootens verfügbar sind (ACTION=change):

```
[2015-04-25 00:33:35] [INFO ] ACTION=change SUBSYSTEM=block DEVNAME=vda1 DEVPATH=/devices/pci0000:00/0000:00:08.0/virtio4/block/vda/vda1 MDEV=vda1
[2015-04-25 00:33:35] [INFO ] TYPE: vfat
[2015-04-25 00:33:35] [INFO ] UUID: 442e-93ba
[2015-04-25 00:33:35] [INFO ] mount point: /media/442e-93ba
[2015-04-25 00:33:35] [ERROR ] /dev/vda1 already mounted on /boot, giving up
```

## 4. Pakete

```
[2015-04-25 00:33:35] [INFO] ] ACTION=change SUBSYSTEM=block DEVNAME=vda2 DEVPATH=/devices/pci0000:00/0000:00:08.0/virtio4/block/vda/vda2 MDEV=vda2
[2015-04-25 00:33:35] [INFO] ] TYPE: ext3
[2015-04-25 00:33:35] [INFO] ] UUID: 77ab35b3-029e-42c9-93a0-d197c01e6e89
[2015-04-25 00:33:35] [INFO] ] mount point: /media/77ab35b3-029e-42c9-93a0-d197c01e6e89
[2015-04-25 00:33:35] [INFO] ] /dev/vda2: clean, 671/26208 files, 57544/104420 blocks
[2015-04-25 00:33:35] [NOTICE] ] /dev/vda2 mounted on /media/77ab35b3-029e-42c9-93a0-d197c01e6e89
[2015-04-25 00:33:36] [INFO] ] ACTION=change SUBSYSTEM=block DEVNAME=vda3 DEVPATH=/devices/pci0000:00/0000:00:08.0/virtio4/block/vda/vda3 MDEV=vda3
[2015-04-25 00:33:36] [INFO] ] TYPE: ext3
[2015-04-25 00:33:36] [INFO] ] UUID: 1580b80c-92b1-4492-abfa-92a12a7d2027
[2015-04-25 00:33:36] [INFO] ] mount point: /media/1580b80c-92b1-4492-abfa-92a12a7d2027
[2015-04-25 00:33:36] [ERROR] ] /dev/vda3 already mounted on /data, giving up
[2015-04-25 00:33:36] [INFO] ] ACTION=change SUBSYSTEM=block DEVNAME=vdb1 DEVPATH=/devices/pci0000:00/0000:00:0a.0/virtio5/block/vdb/vdb1 MDEV=vdb1
[2015-04-25 00:33:36] [INFO] ] TYPE: ext3
[2015-04-25 00:33:36] [INFO] ] UUID: 4c1a03e1-3a0c-4835-88dc-a51879def464
[2015-04-25 00:33:36] [INFO] ] mount point: /mnt/extra
[2015-04-25 00:33:36] [ERROR] ] /dev/vdb1 already mounted on /mnt/extra, giving up
[2015-04-25 00:33:36] [INFO] ] ACTION=change SUBSYSTEM=block DEVNAME=vdc1 DEVPATH=/devices/pci0000:00/0000:00:1f.0/virtio6/block/vdc/vdc1 MDEV=vdc1
[2015-04-25 00:33:36] [INFO] ] TYPE: vfat
[2015-04-25 00:33:36] [INFO] ] UUID: ba6e-9ebd
[2015-04-25 00:33:36] [INFO] ] mount point: /media/ba6e-9ebd
[2015-04-25 00:33:36] [INFO] ] fsck.fat 3.0.26 (2014-03-07)
[2015-04-25 00:33:36] [INFO] ] /dev/vdc1: 0 files, 0/32672 clusters
[2015-04-25 00:33:36] [NOTICE] ] /dev/vdc1 mounted on /media/ba6e-9ebd
```

Zwei Datenpartitionen wurden eingehängt (`/dev/vda2` und `/dev/vdc1`), davon wurden beide nicht via `OPT_EXTMOUNT` konfiguriert und somit unterhalb von `/media` eingehängt. Die verbliebenen drei Datenpartitionen `/dev/vda1`, `/dev/vda3` und `/dev/vdb1` wurden bereits von anderen Boot-Skripten eingehängt und entsprechen der Boot- und der Datenpartition sowie einer benutzerdefinierten `OPT_EXTMOUNT`-Datenpartition.

Jetzt werden `/dev/vdb1` und `/dev/vdc1` ausgehängt (`ACTION=remove`; die Warnung, dass `/dev/vdb1` beim Aushängen nicht in der Volumen-Datenbank gefunden wurde, ist harmlos und weist darauf hin, dass diese Datenpartition bereits während des Bootens von `OPT_EXTMOUNT` und nicht von `OPT_AUTOMOUNT` eingehängt wurde)...

```
[2015-04-25 00:34:52] [INFO] ] ACTION=remove SUBSYSTEM=block DEVNAME=vdb1 DEVPATH=/devices/pci0000:00/0000:00:0a.0/virtio5/block/vdb/vdb1 MDEV=vdb1
[2015-04-25 00:34:52] [WARNING] ] /dev/vdb1 not found in volume database
[2015-04-25 00:34:52] [INFO] ] mount point: /mnt/extra
[2015-04-25 00:34:52] [NOTICE] ] /dev/vdb1 unmounted from /mnt/extra
[2015-04-25 00:34:55] [INFO] ] ACTION=remove SUBSYSTEM=block DEVNAME=vdc1 DEVPATH=/devices/pci0000:00/0000:00:1f.0/virtio6/block/vdc/vdc1 MDEV=vdc1
[2015-04-25 00:34:55] [INFO] ] UUID: ba6e-9ebd
[2015-04-25 00:34:55] [INFO] ] mount point: /media/ba6e-9ebd
[2015-04-25 00:34:55] [NOTICE] ] /dev/vdc1 unmounted from /media/ba6e-9ebd
```

...und in umgekehrter Reihenfolge wieder eingehängt (`ACTION=add`):

```
[2015-04-25 00:35:14] [INFO] ] ACTION=add SUBSYSTEM=block DEVNAME=vdb1 DEVPATH=/devices/pci0000:00/0000:00:0b.0/virtio5/block/vdb/vdb1 MDEV=vdb1
[2015-04-25 00:35:14] [INFO] ] TYPE: vfat
[2015-04-25 00:35:14] [INFO] ] UUID: ba6e-9ebd
[2015-04-25 00:35:14] [INFO] ] mount point: /media/ba6e-9ebd
[2015-04-25 00:35:15] [INFO] ] fsck.fat 3.0.26 (2014-03-07)
[2015-04-25 00:35:15] [INFO] ] /dev/vdb1: 0 files, 0/32672 clusters
[2015-04-25 00:35:15] [NOTICE] ] /dev/vdb1 mounted on /media/ba6e-9ebd
[2015-04-25 00:35:18] [INFO] ] ACTION=add SUBSYSTEM=block DEVNAME=vdc1 DEVPATH=/devices/pci0000:00/0000:00:0c.0/virtio6/block/vdc/vdc1 MDEV=vdc1
[2015-04-25 00:35:18] [INFO] ] TYPE: ext3
[2015-04-25 00:35:18] [INFO] ] UUID: 4c1a03e1-3a0c-4835-88dc-a51879def464
[2015-04-25 00:35:18] [INFO] ] mount point: /mnt/extra
[2015-04-25 00:35:18] [INFO] ] /dev/vdc1: recovering journal
[2015-04-25 00:35:18] [INFO] ] /dev/vdc1: clean, 11/16384 files, 7477/65488 blocks
[2015-04-25 00:35:18] [NOTICE] ] /dev/vdc1 mounted on /mnt/extra
```

Das “unsaubere” Aushängen des ext3-Dateisystems auf `/dev/vdc1` hat zu einer “recovering journal”-Meldung beim Einhängen geführt, die aber nicht kritisch ist, da keine weiteren Fehler gefunden wurden.

### 4.10.5. OPT\_HDSLEEP – automatisches Abschalten für Festplatten einstellen

Eine Festplatte kann sich automatisch abschalten, wenn eine bestimmte Zeit ohne Aktivität verstreicht. Damit benötigt die Platte kaum noch Strom und macht keine Geräusche mehr. Wenn ein Zugriff auf die Festplatte erfolgt, läuft sie automatisch wieder an.

Nicht alle Festplatten vertragen häufiges Wiederanlaufen. Daher sollte man die Zeit nicht zu klein wählen. Ältere IDE-Platten bieten diese Funktion erst gar nicht an. Bei Flash-Medien ist diese Einstellung nicht sinnvoll und auch nicht notwendig.

**HDSLEEP\_TIMEOUT** Diese Variable legt fest, nach welcher Zeit ohne Zugriff die Festplatte in den Power-Down-Modus gehen soll. Dann schaltet sie sich automatisch nach der Wartezeit aus und beim nächsten Zugriff wieder ein. Hierbei sind Wartezeiten in Minutenabständen von einer bis 20 Minuten sowie in Abständen von 30 Minuten von einer Halben bis zu fünf Stunden möglich. Eine Wartezeit von 21 oder 25 Minuten z.B. wird also auf 30 Minuten aufgerundet. Manche Festplatten ignorieren zu hohe Werte und stoppen dann schon nach einigen Minuten. Bitte unbedingt die korrekte Funktion durchtesten, da dies sehr von der jeweiligen Hardware abhängig ist!

```
HDSLEEP_TIMEOUT='2'                # wait 2 minutes until power down
```

#### 4.10.6. OPT\_RECOVER – Notfalloption

Diese Variable legt fest, ob Funktionen zur Erstellung einer Notfalloption verfügbar sind. Wenn die Option aktiviert ist wird der Befehl “mkrecover.sh” mit auf den Router übertragen. Mit diesem kann an der Kommandokonsole durch einfachen Aufruf die Notfallinstallation aktiviert werden. Beim installierten Paket “HTTPD” kann die Übertragung der aktuell laufenden Installation in eine Notfallinstallation im Menü Recover durchgeführt werden.

Um die Notfallinstallation zu nutzen, ist beim nächsten Reboot im Bootmenü die Auswahl Recover auszuwählen.

```
OPT_RECOVER='yes'
```

#### 4.10.7. OPT\_HDDRV - Treiber für Festplattencontroller

Mit OPT\_HDDRV='yes' können eventuell benötigte zusätzliche Treiber aktiviert und installiert werden. Für IDE und SATA ist es in der Regel nicht nötig einen speziellen Treiber zu laden, da diese bereits vom Paket Base geladen werden.

**HDDRV\_N** Die Anzahl der Treiber, die geladen werden sollen, wird hier eingestellt.

**HDDRV\_x** Mit HDDRV\_1 usw. werden die entsprechenden Treiber für die verwendeten Host-Adapter ausgewählt. Eine Liste der unterstützten Hostadapter ist in der initialen Konfigurationsdatei enthalten.

**HDDRV\_x\_OPTION** Mit HDDRV\_x\_OPTION können Optionen übergeben werden, die einige Treiber zum laden benötigen. Dies kann z.B. eine IO-Adresse sein. Bei den meisten Treibern kann diese Variable einfach leer gelassen werden.

Im [Anhang](#) (Seite 416) finden Sie eine Übersicht der Fehler, die bei Festplatten und CompactFlash am häufigsten auftreten.

Beispiel 1: Zugriff auf SCSI-Festplatte an einem Adaptec 2940

```
OPT_HDDRV='yes'                # install Drivers for Harddisk: yes or no
HDDRV_N='1'                    # number of HD drivers
HDDRV_1='aic7xxx'              # various aic7xxx based Adaptec SCSI
HDDRV_1_OPTION=''              # no need for options yet
```

Beispiel 2: Beschleunigter IDE-Zugriff beim PC-Engines ALIX

```
OPT_HDDRV='yes'           # install Drivers for Harddisk: yes or no
HDDRV_N='1'               # number of HD drivers
HDDRV_1='pata_amd'        # AMD PCI IDE/ATA driver (e.g. ALIX)
HDDRV_1_OPTION=''         # no need for options yet
```

## 4.11. HTTPD - Status-Webserver

### 4.11.1. OPT\_HTTPD - Mini-Webserver als Statusmonitor

Wer aus irgendeinem Grund keine Möglichkeit hat, den IMONC zu benutzen, weil er z.B. einen Mac benutzt, kann den Webserver benutzen, um den Status des fli4l-Routers abzurufen oder zu ändern. Mit `OPT_HTTPD='yes'` kann man den Statusmonitor verwenden.

Um den Status abzurufen, muss man in seinen Browser eine der folgenden Adressen eingeben:

```
http://fli4l/
http://fli4l.domain.lan/
http://192.168.6.1/
```

Hat der fli4l-Router einen abweichenden Namen, muss dieser statt "fli4l" verwendet werden. Dies gilt auch für den Domain-Namen und die obige IP-Adresse. Hat man den Webserver auf einen anderen Port gelegt (per `HTTPD_PORT`), muss man diesen mit angeben:

```
http://fli4l:81/
```

Es wird seit der Version 2.1.12 eine Login-Seite angezeigt, die nicht passwortgeschützt ist. Die passwortgeschützten Seiten befinden sich im Unterverzeichnis `admin`, also beispielsweise:

```
http://fli4l.domain.lan/admin/
```

Der Webserver lässt sich über folgende Variablen anpassen:

**HTTPD\_GUI\_LANG** Hiermit wird die Sprache eingestellt, in der das Webinterface dargestellt werden soll. Wird hier 'auto' eingetragen, wird die Spracheinstellung der Variablen `LOCALE` (in der `base.txt`) verwendet.

**HTTPD\_LISTENIP** Der Webserver bindet sich normalerweise an eine sogenannte Wildcard-Adresse, so dass er auf einem beliebigen Interface angesprochen werden kann. Soll er sich nur an eine IP-Adresse binden, so kann es mit diesem Parameter eingestellt werden. Dazu die IP-Adresse wie folgt eintragen: `IP_NET_x_IPADDR`. Normalerweise bleibt dieser Parameter leer, damit die Standardeinstellung (ansprechbar auf einer beliebigen IP) greift.

Dieser Parameter dient lediglich dazu, den `httpd` nur an eine IP zu binden, so dass sich andere Instanzen an die anderen IPs des Routers binden können. Er kann nicht ohne weiteres dazu genutzt werden, den Zugang einzelner Subnetze zum Webinterface des Routers zu sperren. Dazu benötigt man weiterhin die Hilfe des Paketfilters.

Es ist auch möglich, hier durch Leerzeichen getrennt mehrere IP anzugeben.

**HTTPD\_PORT** Soll der Webserver auf einem anderen Port laufen als 80, so ist dieser Wert anzupassen. Das ist normalerweise nicht zu empfehlen, da dann z.B. mit `http://fi4l:81/` auf den Webserver zugegriffen werden muß.

**HTTPD\_PORTFW** Setzt man diese Variable auf 'yes', kann man über das Webinterface Änderungen an der Portweiterleitung vornehmen. Es können Regeln gelöscht und hinzugefügt werden, Änderungen werden sofort wirksam. Änderungen an den Regeln gelten nur für die Laufzeit des Routers. Wird der Router neu gestartet, sind die Änderungen weg.

Diese Variable hat einen Defaultwert von 'yes'.

**HTTPD\_ARPING** Der Webserver stellt den Online-Zustand der mit `HOST_x` aufgelisteten Hosts dar. Dazu verwendet er den "*Arp-Cache*", ein Zwischenspeicher der die Adressen der lokalen Hosts zwischenspeichert. Hat ein Rechner lange nicht mehr mit dem Router kommuniziert, verschwindet seine Adresse aus dem "*Arp-Cache*" und der Host scheint aus zu sein. Will man den "*Arp-Cache*" aktuell halten (also das rausfallen eigentlich nicht benötigter Einträge verhindern), kann man `HTTPD_ARPING` auf 'yes' setzen.

**HTTPD\_ARPING\_IGNORE\_N** Legt die Anzahl der zu Ignorierenden Einträge fest

**HTTPD\_ARPING\_IGNORE\_x** IP-Adresse oder Name des Hosts der nicht bei den ARPING-Test geprüft werden soll. Dies kann z.B. sinnvoll sein, bei Hosts die durch die regelmäßigen Netzwerkpakete Ihren Akku schneller verbrauchen (Handys im WLAN).

#### 4.11.2. Nutzerverwaltung

Der Webserver bietet eine ausgefeilte Benutzerverwaltung:

**HTTPD\_USER\_N** Hiermit wird die Anzahl der Benutzer eingestellt. Wird diese Variable auf 0 gesetzt, wird die Benutzerverwaltung komplett deaktiviert und jeder hat die Möglichkeit, auf den Webserver zuzugreifen.

**HTTPD\_USER\_x\_USERNAME HTTPD\_USER\_x\_PASSWORD HTTPD\_USER\_x\_RIGHTS**

Hier werden Benutzername und Passwort der einzelnen Benutzer eingetragen. Desweiteren wird für jeden Benutzer angegeben, auf welche Funktionen des Webserver er zugreifen darf. Diese Funktion wird mit der Variable `HTTPD_RIGHTS_x` geregelt. Im einfachsten Fall steht dort nur 'all', was bedeutet, dass der entsprechende Benutzer alles darf. Ansonsten hat die Variable den folgenden Aufbau:

```
'bereich1:recht1,recht2,... bereich2:...'
```

Statt für einen Bereich die einzelnen Rechte anzugeben, darf auch hier das Wort "all" eingesetzt werden, was wiederum heißt, das dieser Benutzer in diesem Bereich alle Rechte hat. Dabei gibt es folgende Bereiche und Rechte:

**Bereich "status"** Alles, was im Menü Status zu sehen ist.

**view** Der Benutzer darf alle Menüpunkte aufrufen.

**dial** Der Benutzer darf wählen und aufliegen.

**boot** Der Benutzer darf den Router herunterfahren & neu starten.

**link** Der Benutzer darf Kanalbündlung an- und abschalten.

**circuit** Der Benutzer darf den Circuit wechseln.

**dialmode** Der Benutzer darf den Dialmode (Auto, Manual, Off) ändern.

**contrack** Der Benutzer darf die aktuell über den Router laufenden Verbindungen ansehen.

**dyndns** Der Benutzer darf Log-Meldungen des [DYNDNS](#) (Seite 150) Paketes sehen.

**Bereich "logs"** Alles, was mit Logdateien zu tun hat (Verbindungen, Anrufe, Syslog)

**view** Der Benutzer darf die Logdateien betrachten.

**reset** Der Benutzer darf die Logdateien löschen.

**Bereich "support"** Alles, was nützlich ist, wenn man beispielsweise in der Newsgroup Hilfestellung sucht.

**view** Der Benutzer darf die Links zur Doku, fli4l-Webseite, usw. abrufen

**systeminfo** Der Benutzer darf detaillierte Informationen zur Konfiguration und zum aktuellen Status des Routers (z. B.: Firewall) abfragen.

Hier noch einige Beispiele:

**HTTPD\_USER\_1\_RIGHTS='all'** Diese Angabe erlaubt einem Benutzer alles!

**HTTPD\_USER\_2\_RIGHTS='status:view logs:view support:all'** Dieser Benutzer darf sich zwar alles ansehen, aber nichts ändern.

**HTTPD\_USER\_3\_RIGHTS='status:view,dial,link'** Dieser Benutzer darf sich den Status der Internetverbindung ansehen, wählen und Kanalbündelung ein- und ausschalten.

**HTTPD\_USER\_4\_RIGHTS='status:all'** Dieser Benutzer darf alles mit der Internetverbindung machen und neu starten (natürlich auch herunterfahren). Er darf aber nicht die Logdateien sehen oder löschen, die Timetable darf er auch nicht sehen...

### 4.11.3. OPT\_OAC - Online Access Control

**OPT\_OAC** (optionale Variable)

Aktiviert das Modul 'Online Access Control'. Hierüber kann der Internet-Zugang jedes im Paket [dns\\_dhcp](#) (Seite 131) konfigurierten Rechners selektiv deaktiviert werden.

Es gibt auch ein Kommandozeilen-Tool, welches die Steuerung über andere Pakete wie z.B. EasyCron möglich macht:

```
/usr/local/bin/oac.sh
```

Die Optionen werden beim Aufruf angezeigt.

**OAC\_WANDEVICE** (optionale Variable)

Schränkt die Online Zugangssperre auf Verbindungen über dieses Netzwerkdevice ein. z.B. 'pppoe'

**OAC\_INPUT** (optionale Variable)

Bietet Schutz vor der Umgehung via Proxy.

OAC\_INPUT='default' sperrt die konfigurierten Ports von: Privoxy, Squid, Tor, SS5, Transproxy.

OAC\_INPUT='tcp:8080 tcp:3128' sperrt TCP Port 8080 und 3128. Dies ist eine Space-separierte Liste an zu sperrenden Ports mit dazugehörigem Protokoll (udp, tcp). Fehlt das Protokoll, werden udp und tcp Ports gesperrt.

Weglassen dieser Variable oder Inhalt 'no' deaktiviert die Funktion.

**OAC\_ALL\_INVISIBLE** (optionale Variable)

Schaltet die Gesamtübersicht aus, wenn mindestens eine sichtbare Gruppe existiert. Existiert nicht mindestens eine sichtbare Gruppe, so hat diese Variable keine Wirkung.

**OAC\_LIMITS** (optionale Variable)

Gibt eine durch Leerzeichen getrennte Liste der Zeitlimits an, die zur Auswahl stehen. Die Limits werden in Minuten angegeben. Damit kann eine zeitlich limitierte Sperre oder Freigabe erreicht werden.

Default: '30 60 90 120 180 360 540'

**OAC\_MODE** (optionale Variable)

Mögliche Werte: 'DROP' oder 'REJECT' (default)

**OAC\_GROUP\_N** (optionale Variable)

Anzahl der Clientgruppen. Dient der Übersichtlichkeit, erlaubt aber auch über das Web-Interface eine gesamte Gruppe gesammelt freizugeben oder zu sperren.

**OAC\_GROUP\_x\_NAME** (optionale Variable)

Name der Gruppe - Dieser Name wird im Web-Interface angezeigt und ist auch über die das Kommandozeilenscript 'oac.sh' nutzbar.

**OAC\_GROUP\_x\_BOOTBLOCK** (optionale Variable)

Wenn hier 'yes' steht, werden alle Clients der Gruppe beim Bootvorgang bereits gesperrt. Hilfreich, wenn Rechner idr. gesperrt sein sollen und nur ausnahmsweise nicht.

**OAC\_GROUP\_x\_INVISIBLE** (optionale Variable)

Markiert die Gruppe als unsichtbar. Sinnvoll, wenn einige Rechner vorgesperrt werden sollen aber diese nicht als eigene Gruppe im Web-If sichtbar sein sollen. Das Kommandozeilentool oac.sh kann diese trotzdem ansprechen, wenn man das braucht, z.B. von easycron aus.

**OAC\_GROUP\_x\_CLIENT\_N** (optionale Variable)

Anzahl der Clients in der Gruppe.

**OAC\_GROUP\_x\_CLIENT\_x** (optionale Variable)

Name des Clients wie in HOST\_x\_NAME des Pakets [dns\\_dhcp](#) (Seite 131) definiert.



### **OAC\_BLOCK\_UNKNOWN\_IF\_x** (optionale Variable)

Liste der in base.txt definierten Interfaces, auf welchen nur in dns\_dhcp.txt definierte Hosts ins Internet dürfen. Nicht-definierte Hosts sind hier damit generell gesperrt.

## **4.12. HWSUPP - Unterstützung von Hardware**

### **4.12.1. Beschreibung**

Das Paket stellt die Unterstützung für die Nutzung spezieller Hardwarekomponenten bereit. Unterstützte Hardwarekomponenten/-elemente:

- Temperatursensoren
- LEDs
- Spannungssensoren
- Lüfterdrehzahlen
- Taster
- Watchdog
- VPN-Karten

Unterstützung gibt es für die folgende Systeme/Mainboards/VPN-Karten:

- Standard PC-Hardware
  - LEDs einer PC-Tastatur
- ACPI-PC-Hardware
- Embedded Systeme
  - AEWIN SCB6971
  - Fujitsu Siemens Futro S200
  - Fujitsu Siemens Futro S900
  - PC Engines ALIX
  - PC Engines APU
  - PC Engines WRAP
  - Soekris net4801
  - Soekris net5501
- Mainboards
  - Commell LE-575
  - GigaByte GA-M521-S3
  - GigaByte GA-N3150N-D3V
  - LEX CV860A

- MSI MS-9803
- SuperMicro PDSME
- SuperMicro X7SLA
- Tyan S5112
- WinNet PC640
- WinNet PC680
- VPN Karten (PCI, miniPCI and miniPCIe)
  - vpn1401 vpn1411

### 4.12.2. Konfiguration des Paketes HWSUPP

Die Konfiguration erfolgt, wie bei allen fli4l Paketen, durch Anpassung der Datei Pfad/fli4l-4.0.0-trunk-rpi-r60784/<config>/hwsupp.txt an die eigenen Anforderungen.

**OPT\_HWSUPP** Die Einstellung 'no' deaktiviert das OPT\_HWSUPP vollständig. Es werden keine Änderungen am fli4l Archiv rootfs.img bzw. dem Archiv opt.img vorgenommen. Weiterhin überschreibt das OPT\_HWSUPP grundsätzlich keine anderen Teile der fli4l Installation.

Um OPT\_HWSUPP zu aktivieren, ist die Variable OPT\_HWSUPP auf 'yes' zu setzen.

**HWSUPP\_TYPE** In dieser Konfigurationsvariable wird die zu unterstützende Hardware festgelegt. Folgende Werte stehen zur Verfügung:

- sim
- generic-pc
- generic-acpi
- generic-acpi-coretemp
- aewin-scb6971
- commell-le575
- fsc-futro-s200
- fsc-futro-s900
- gigabyte-ga-m52l-s3
- gigabyte-ga-n3150n-d3v
- lex-cv860a
- msi-ms-9803
- pcengines-alix
- pcengines-apu (APU-1)
- pcengines-apu2 (APU-2)
- pcengines-wrap
- rpi

- soekris-net4801
- soekris-net5501
- supermicro-pdsme
- supermicro-x7sla
- tyan-s5112
- winnet-pc640
- winnet-pc680

**HWSUPP\_WATCHDOG** Die Einstellung 'yes' aktiviert den Watchdog-Daemon falls die gewählte Hardware einen Watchdog besitzt. Durch den Watchdog wird ein hängendes System automatisch neu gestartet werden.

**HWSUPP\_CPUFREQ** Die Einstellung 'yes' aktiviert die Anpassung der Prozessor-Taktfrequenz.

**HWSUPP\_CPUFREQ\_GOVERNOR** Auswahl des CPU-Frequenz-Reglers. Die Auswahl des Reglers steuert das Verhalten der Anpassung der Prozessor-Taktfrequenz. Zur Auswahl stehen:

- performance

Der Prozessor läuft immer mit der maximalen Taktfrequenz.

- ondemand

Die CPU-Frequenz wird an die Rechenleistung angepasst. Dabei kann die CPU-Frequenz u.U. sprunghaft angehoben oder abgesenkt werden.

- conservative

Die CPU-Frequenz wird an die Rechenleistung angepasst. Die CPU-Frequenz wird schrittweise angehoben bzw. abgesenkt.

- powersave

Der Prozessor läuft immer mit der minimalen Taktfrequenz.

- userspace

Der Prozessortakt kann manuell oder von einem Anwenderskript über die sysfs-Variable `/devices/system/cpu/cpu<n>/cpufreq/scaling_setspeed` gesetzt werden.

**HWSUPP\_LED\_N** Definiert die Anzahl der LEDs. Hier sollte die Anzahl der LEDs die die verwendete Hardware bereitstellt stehen.

**HWSUPP\_LED\_x** Definiert die Information, die durch das LED angezeigt werden soll. Folgende Informationen sind möglich:

- ready - Der fli4l-Router ist betriebsbereit<sup>4</sup>
- online - der fli4l-Router ist mit den Internet verbunden
- trigger - Anzeige wird durch einen LED-Trigger gesteuert
- user - Anzeige wird durch ein Benutzerskript gesteuert

Die Liste der möglichen Information kann durch andere Pakete erweitert werden. So ist bei geladenem WLAN-Paket z.B. die Anzeige

- wlan - das WLAN ist aktiviert

möglich.

Im Anhang [B.10](#) finden sich Hinweise für Paket-Entwickler wie eine solche Erweiterung anzulegen ist.

**HWSUPP\_LED\_x\_DEVICE** Gibt das LED-Device an.

Hier wird entweder ein LED-Device eingetragen (zu finden unter `/sys/class/leds/` im Dateisystem des Routers) oder eine GPIO<sup>5</sup>-Nummer.

Eine Liste gültiger Namen der LED-Devices für den jeweiligen HWSUPP\_TYPE findet sich im Anhang [“Verfügbare LED-Devices”](#) (Seite 418).

Die GPIO-Nummer muss im Format `gpio::x` eingegeben werden. Wenn man ein GPIO eingetragen, so wird das dazugehörige LED-Device automatisch angelegt. Durch Voranstellen von `/` wird die Funktionsweise des GPIO invertiert.

Beispiele:

```
HWSUPP_LED_1_DEVICE='apu::1'
HWSUPP_LED_2_DEVICE='gpio::237'
HWSUPP_LED_3_DEVICE='/gpio::245'
HWSUPP_LED_4_DEVICE='led0'
```

**HWSUPP\_LED\_PARAM** Definiert Parameter für die ausgewählte LED Anzeige.

Je nach Auswahl in HWSUPP\_LED\_x hat HWSUPP\_LED\_x\_PARAM eine unterschiedliche Bedeutung.

Ist HWSUPP\_LED\_x='trigger', so ist der Name des LED-Triggers, der die Ansteuerung der LED kontrolliert, in HWSUPP\_LED\_x\_PARAM einzutragen.

Die verfügbaren Trigger können mit dem Shell-Kommando `cat /sys/class/leds/*/trigger` angezeigt werden.

Neben den Triggern die von z.B. netfilter oder Hardwaretreibern wie ath9k erzeugt werden, können weitere Trigger-Module über HWSUPP\_DRIVER\_x geladen werden.

Beispiele:

```
HWSUPP_LED_1='trigger'
HWSUPP_LED_1_PARAM='heartbeat'
HWSUPP_LED_2='trigger'
HWSUPP_LED_2_PARAM='netfilter-ssh'
```

---

<sup>4</sup>Ist HWSUPP\_LED\_x='ready', so wird der Bootfortschritt durch eine Blink-folge angezeigt (siehe Anhang [B.8](#)).

<sup>5</sup>Ein GPIO (General Purpose Input/Output) ist ein Kontaktstift an einem integrierten Schaltkreis, dessen Verhalten durch Programmierung bestimmbar ist, unabhängig, ob als Ein- oder Ausgabekontakt.

#### 4. Pakete

Ist `HWSUPP_LED_x='user'`, so ist in `HWSUPP_LED_PARAM` ein gültiger Skriptname inclusive Pfad einzutragen.

Beispiel:

```
HWSUPP_LED_1='user'
HWSUPP_LED_1_PARAM='/usr/local/bin/myledscript'
```

Ist `HWSUPP_LED_x='wlan'`, so definiert `HWSUPP_LED_PARAM` ein oder mehrere WLAN Devices, deren Zustand angezeigt wird. Mehrere WLAN Devices sind durch Leerzeichen zu trennen.

Wird der Zustand mehrerer WLAN Devices mit einer LED Angezeigt, so hat die LED folgende Bedeutung:

- aus - alle WLAN Devices sind inaktiv
- blinkt - ein Teil der WLAN Devices ist aktiv
- an - alle WLAN Devices sind aktiv

Beispiel:

```
HWSUPP_LED_1='wlan'
HWSUPP_LED_1_PARAM='wlan0 wlan1'
```

**HWSUPP\_BOOT\_LED** Definiert eine LED die während des Bootvorgangs den Fortschritt durch eine Blinkfolge angezeigt.

Wenn für eine LED `HWSUPP_LED_x='ready'` gesetzt ist so hat diese Einstellung Vorrang und `HWSUPP_BOOT_LED` wird ignoriert.

**HWSUPP\_BUTTON\_N** Definiert die Anzahl der BUTTONs. Hier sollte die Anzahl der Taster die die verwendete Hardware bereitstellt stehen.

**HWSUPP\_BUTTON\_x** Definiert die Aktion die durch drücken des Tasters durchgeführt werden soll. Folgende Aktionen sind möglich:

- reset - Startet den fli4l-Router neu
- online - Baut die Internetverbindung auf bzw. beendet diese
- user - Ein User-Script wird ausgeführt

Die Liste der möglichen Aktionen kann durch andere Pakete erweitert werden. So ist bei geladenem WLAN-Paket z.B. die Aktion

- wlan - WLAN aktivieren bzw. deaktivieren

möglich.

**HWSUPP\_BUTTON\_x\_DEVICE** Gibt das Button-Device an. Hier gibt es zwei Möglichkeiten. Zum einen kann eine GPIO-Nummer eingetragen werden. Zum anderen kann ein so genannter Input-Pfad angegeben werden, der später über das evdev-Subsystem

ausgelesen wird. Die zweite Möglichkeit ist, wenn möglich, immer vorzuziehen, weil die GPIO-Indizes nicht unbedingt über Kernelgrenzen hinweg stabil bleiben.

Die GPIO-Nummer muss im Format `gpio::x` eingegeben werden. Normalerweise wird angenommen, dass die GPIO-Pins “active-low” sind, d. h. dass sie den Wert 0 annehmen, wenn ein Taster gedrückt wird, und 1, wenn der Taster nicht gedrückt ist. Liegt der umgekehrte Fall “active-high” vor (also 1 bei gedrücktem und 0 bei nicht gedrücktem Taster), kann dies durch Voranstellen von `/` angezeigt werden.

Der Input-Pfad muss im Format `evdev:<Pfad>` eingegeben werden. In diesem Fall muss mit Hilfe der Variable `HWSUPP_BUTTON_x_DEVICE_KEY` spezifiziert werden, welche Taste verarbeitet werden soll. Dies ist nötig, weil im Gegensatz zur Anbindung via GPIO-Pin ein einziges evdev-Gerät viele verschiedene Buttons kapseln kann. Eine Übersicht der Tasten findet sich im Anhang “[Tasten-Codes](#)” (Seite 422).

Eine Liste der vordefinierten Input-Pfade für den jeweiligen `HWSUPP_TYPE` findet sich im Anhang “[Verfügbare Button-Devices](#)” (Seite 419).

Beispiele:

```
HWSUPP_BUTTON_1_DEVICE='/gpio::237' # GPIO-Pin #237, active-high
HWSUPP_BUTTON_2_DEVICE='evdev:isa0060/serio0/input0' # AT-Tastatur,
HWSUPP_BUTTON_2_DEVICE_KEY='88' # F12-Taste
```

**HWSUPP\_BUTTON\_x\_PARAM** Definiert Parameter für die ausgewählte Aktion.

Je nach Wert in `HWSUPP_BUTTON_x` hat `HWSUPP_BUTTON_x_PARAM` eine unterschiedliche Funktion.

Ist `HWSUPP_BUTTON_x='user'`, so definiert `HWSUPP_BUTTON_x_PARAM` ein Script das beim Drücken des Tasters ausgeführt werden soll.

Beispiel:

```
HWSUPP_BUTTON_1='user'
HWSUPP_BUTTON_2_WLAN='/usr/local/bin/myscript'
```

Ist `HWSUPP_BUTTON_x_ACTION='wlan'`, so sind in `HWSUPP_BUTTON_x_PARAM` das oder die WLAN Devices einzutragen, die durch Drücken des Tasters aktiviert bzw. deaktiviert werden. Mehrere WLAN Devices sind durch Leerzeichen zu trennen.

Beispiel:

```
HWSUPP_BUTTON_2='wlan'
HWSUPP_BUTTON_2_WLAN='wlan0 wlan1'
```

### 4.12.3. Experten-Einstellungen

Die folgenden Einstellungen sollten nur gemacht werden, wenn man genau weiß

- welche Hardware man hat und welche zusätzlichen Treiber man dafür benötigt
- an welchen Adressen welche I<sup>2</sup>C-Geräte<sup>6</sup> liegen.

Nach dem Aktivieren der Experteneinstellungen erhält man eine Warnung beim mkfli4l Bau.

**HWSUPP\_DRIVER\_N** Anzahl der zusätzlich zu ladenden Treiber. Die Treiber in **HWSUPP\_DRIVER\_x** werden in der angegebenen Reihenfolge geladen.

**HWSUPP\_DRIVER\_x** Name des Treibers (ohne Dateiendung `.ko`).

Beispiel:

```
HWSUPP_DRIVER_N='2'
HWSUPP_DRIVER_1='i2c-piix4'      # I2C Bus Treiber
HWSUPP_DRIVER_2='gpio-pcf857x'  # I2C GPIO Expander
```

**HWSUPP\_I2C\_N** Anzahl der zu ladenden I<sup>2</sup>C-Geräte.

I<sup>2</sup>C unterstützt keine PnP-Mechanismen. Daher sind für jedes zu ladende I<sup>2</sup>C-Gerät die Busnummer, die Geräteadresse und der Gerätetyp anzugeben.

**HWSUPP\_I2C\_x\_BUS** I<sup>2</sup>C-Busnummer an der das zu ladende Gerät angeschlossen ist.

Die Busnummer ist im Format `i2c-x` anzugeben.

**HWSUPP\_I2C\_x\_ADDRESS** I<sup>2</sup>C-Busadresse des Geräts.

Die Adresse ist als Hexadezimalzahl im Bereich von `0x03` bis `0x77` anzugeben.

**HWSUPP\_I2C\_x\_DEVICE** Der Typ des I<sup>2</sup>C-Geräts der vom einem zuvor geladenen Treiber erkannt wird.

Beispiel:

```
HWSUPP_I2C_N='1'
HWSUPP_I2C_1_BUS='i2c-1'
HWSUPP_I2C_1_ADDRESS='0x38'
HWSUPP_I2C_1_DEVICE='pcf8574a' # Unterstützt von gpio-pcf857x Treiber
```

### 4.12.4. Unterstützung von VPN-Karten

**OPT\_VPN\_CARD** Die Einstellung `'no'` deaktiviert das **OPT\_VPN\_CARD** vollständig. Es werden keine Änderungen am fli4l Archiv `rootfs.img` bzw. dem Archiv `opt.img` vorgenommen. Weiterhin überschreibt das **OPT\_VPN\_CARD** grundsätzlich keine anderen Teile der fli4l Installation.

Um **OPT\_VPN\_CARD** zu aktivieren, ist die Variable **OPT\_VPN\_CARD** auf `'yes'` zu setzen.

---

<sup>6</sup>Ein I<sup>2</sup>C-Bus oder SMBus ist ein serieller Bus der im PC z.B. zum Auslesen von Temperatur-Sensoren verwendet wird. Vielfach ist der I<sup>2</sup>C-Bus oder SMBus auf einer Stiftleiste verfügbar und kann für eigene Hardwareerweiterungen genutzt werden.

**VPN\_CARD\_TYPE** In dieser Konfigurationsvariable wird der zu unterstützende VPN Beschleuniger festgelegt. Folgende Werte stehen zur Verfügung:

- hifn7751 - Soekris vpn1401 und vpn1411
- hifnhipp

### 4.13. IPv6 - Unterstützung von IPv6-Tunneln durch IPv4-Netzwerke

#### 4.13.1. Einleitung

Dieses Paket unterstützt das Aufbauen von Tunneln zu IPv6-Anbietern. Dies ist immer dann interessant bzw. nötig, wenn man gern IPv6-Verbindungen ins Internet nutzen möchte, der eigene Internet-Anbieter aber keine native IPv6-Unterstützung anbietet. Momentan erlaubt das Paket die Nutzung von so genannten 6in4-Tunneln, wie sie etwa der Anbieter "Hurricane Electric" unterstützt. Andere Technologien (AYIYA, 6to4, Teredo) werden zur Zeit nicht unterstützt.

Sie müssen für die Nutzung von Tunneln die generelle IPv6-Unterstützung mit Hilfe der Variable `OPT_IPV6='yes'` aktivieren.

#### 4.13.2. Konfiguration

##### Tunnel-Konfiguration

**Wichtig:** *Dieser Abschnitt ist falsch, weil veraltet! Für die Nutzung von 6in4-Tunneln müssen Circuits vom Typ "tun6in4" konfiguriert werden! Schauen Sie sich hierzu die Beispiel-Konfigurationen in der config/ipv6.txt an!*

Dieser Abschnitt stellt die Konfiguration von 6in4-IPv6-Tunneln vor. Ein solcher Tunnel bietet sich an, wenn der eigene Internet-Anbieter kein IPv6 von Haus aus unterstützt. In diesem Fall wird mit einem bestimmten Internet-Host eines Tunnel-Brokers, dem so genannten PoP (Point of Presence), via IPv4 eine bidirektionale Verbindung aufgebaut, über die dann alle IPv6-Pakete verpackt geroutet werden (deswegen 6 "in" 4, weil die IPv6-Pakete innerhalb von IPv4-Paketen gekapselt werden).<sup>7</sup> Damit das funktioniert, muss zum einen der Tunnel aufgebaut und zum anderen der Router so konfiguriert werden, dass die IPv6-Pakete, die ins Internet sollen, auch über den Tunnel geroutet werden. Der erste Teil wird in diesem Abschnitt konfiguriert, der zweite Teil wird im nächsten Abschnitt beschrieben.

**IPV6\_TUNNEL\_N** Diese Variable enthält die Anzahl der aufzubauenden 6in4-Tunnel.

Beispiel: `IPV6_TUNNEL_N='1'`

**IPV6\_TUNNEL\_x\_TYPE** Diese Variable bestimmt den Typ des Tunnels. Momentan werden die Werte "raw" für "rohe" Tunnel, "static" für statische Tunnel und "he" für Tunnel des Anbieters Hurricane Electric unterstützt. Mehr zu Heartbeat-Tunneln steht im nächsten Absatz.

Beispiel: `IPV6_TUNNEL_1_TYPE='he'`

---

<sup>7</sup>Es handelt sich um das IPv4-Protokoll 41, "IPv6 encapsulation".



**IPV6\_TUNNEL\_x\_DEFAULT** Diese Variable legt fest, ob IPv6-Pakete, die nicht an das lokale bzw. die lokalen Netze adressiert sind, über diesen Tunnel geroutet werden sollen. Es kann nur einen solchen Tunnel geben (weil nur eine Default-Route existieren kann). Mögliche Werte sind “yes” und “no”.

**Wichtig:** *Genau ein Tunnel sollte ein Default-Gateway für nausgehende IPv6-Daten sein, da andernfalls eine Kommunikation mit IPv6-Hosts im Internet nicht möglich ist! Die ausschließliche Verwendung von Nicht-Default-Tunneln ist nur sinnvoll, wenn ausgehende IPv6-Daten über eine separat konfigurierte Default-Route geschickt werden, die nicht mit einem Tunnel zusammenhängt. Siehe hierzu auch die Einleitung zum Unterabschnitt “Routen-Konfiguration” sowie die Beschreibung der Variable IPV6\_ROUTE\_x weiter unten.*

Standard-Konfiguration: `IPV6_TUNNEL_1_DEFAULT='no'`

**IPV6\_TUNNEL\_x\_PREFIX** Diese Variable enthält den IPv6-Subnetzpräfix des Tunnels in CIDR-Notation, d.h. es wird sowohl eine IPv6-Adresse als auch die Länge des Präfixes angegeben. Diese Angabe wird in der Regel vom Tunnelanbieter vorgegeben. Bei Tunnelanbietern, die den Präfix beim Tunnelaufbau jedes Mal neu vergeben, ist diese Angabe unnötig. (Momentan werden solche Anbieter aber noch nicht unterstützt.) Diese Variable muss auch bei rohen (“raw”) Tunneln leer bleiben.

**Wichtig:** *Diese Variable darf leer bleiben, wenn dem Tunnel noch kein Subnetz-Präfix zugewiesen worden ist. Allerdings kann dieser Tunnel dann nicht einem IPv6-Subnetz (IPV6\_NET\_x) zugeordnet werden, weil die IPv6-Adressen im Subnetz nicht berechnet werden können. Sinnvoll ist eine solche Konfiguration also nur übergangsweise, etwa wenn der Tunnel einige Zeit aktiv sein muss, bevor der Tunnelanbieter einem ein Subnetz-Präfix zuweist.*

Beispiele:

```
IPV6_TUNNEL_1_PREFIX='2001:db8:1743::/48'      # /48-Subnetz
IPV6_TUNNEL_2_PREFIX='2001:db8:1743:5e00::/56'  # /56-Subnetz
```

**IPV6\_TUNNEL\_x\_LOCALV4** Diese Variable enthält die lokale IPv4-Adresse des Tunnels oder den Wert ‘dynamic’, wenn die dynamisch zugewiesene IPv4-Adresse des aktiven WAN-Circuits verwendet werden soll. Letzteres ist nur sinnvoll, wenn es sich um einen Heartbeat-Tunnel handelt (siehe IPV6\_TUNNEL\_x\_TYPE weiter unten).

Beispiele:

```
IPV6_TUNNEL_1_LOCALV4='172.16.0.2'
IPV6_TUNNEL_2_LOCALV4='dynamic'
```

**IPV6\_TUNNEL\_x\_REMOTEV4** Diese Variable enthält die entfernte IPv4-Adresse des Tunnels. Diese Angabe wird in der Regel vom Tunnel-Anbieter vorgegeben.

Beispiel (entspricht dem PoP deham01 von Easynet):

#### 4. Pakete

IPV6\_TUNNEL\_1\_REMOTEV4='212.224.0.188'

**Wichtig:** Wenn `PF_INPUT_ACCEPT_DEF` auf “no” steht, d.h. wenn die IPv4-Firewall manuell konfiguriert wird, dann wird eine Regel benötigt, die alle IPv6-in-IPv4-Pakete (IP-Protokoll 41) vom Tunnelendpunkt akzeptiert. Für den o.g. Tunnelendpunkt sähe die entsprechende Regel wie folgt aus:

`PF_INPUT_x='prot:41 212.224.0.188 ACCEPT'`

**IPV6\_TUNNEL\_x\_LOCALV6** Diese Variable legt die lokale IPv6-Adresse des Tunnels inklusive verwendeter Netzmaske in CIDR-Notation fest. Diese Angabe wird vom Tunnelanbieter vorgegeben. Bei Tunnelanbietern, welche die Tunnelendpunkte beim Tunnelaufbau jedes Mal neu vergeben, ist diese Angabe unnötig. (Momentan werden solche Anbieter aber noch nicht unterstützt.)

Beispiel: `IPV6_TUNNEL_1_LOCALV6='2001:db8:1743::2/112'`

**IPV6\_TUNNEL\_x\_REMOTEV6** Diese Variable legt die entfernte IPv6-Adresse des Tunnels fest. Diese Angabe wird vom Tunnelanbieter vorgegeben. Eine Netzmaske wird nicht benötigt, da sie der Variable `IPV6_TUNNEL_x_LOCALV6` entnommen wird. Bei Tunnelanbietern, welche die Tunnelendpunkte beim Tunnelaufbau jedes Mal neu vergeben, ist diese Angabe unnötig. (Momentan werden solche Anbieter aber noch nicht unterstützt.)

Beispiel: `IPV6_TUNNEL_1_REMOTEV6='2001:db8:1743::1'`

**IPV6\_TUNNEL\_x\_DEV** (optional) Diese Variable enthält den Namen der zu erstellenden Tunnel-Netzwerkschnittstelle. Verschiedene Tunnel müssen unterschiedlich benannt werden, damit alles funktioniert. Falls die Variable nicht definiert ist, wird ein Tunnelname automatisch generiert (“v6tun” + Tunnelindex).

Beispiel: `IPV6_TUNNEL_1_DEV='6in4'`

**IPV6\_TUNNEL\_x\_MTU** (optional) Diese Variable enthält die Größe der MTU (Maximum Transfer Unit) in Bytes, d.h. des größten Pakets, das noch getunnelt werden kann. Diese Angabe wird in der Regel vom Tunnelanbieter vorgegeben. Die Standard-Einstellung, falls nichts angegeben wird, lautet “1280” und sollte mit allen Tunneln funktionieren.

Standard-Konfiguration: `IPV6_TUNNEL_1_MTU='1280'`

Einige Tunnelanbieter verlangen, dass über den Tunnel permanent ein Lebenszeichen vom Router an den Anbieter gesandt wird, um zu verhindern, dass ein Host einen Tunnel in Anspruch nimmt, obwohl er ihn nicht nutzt. Dazu wird ein so genanntes Heartbeat-Protokoll (dt. “Herzschlag”) verwendet. Zusätzlich verlangen Anbieter in der Regel eine erfolgreiche Anmeldung mit Benutzernamen und Passwort, um Missbrauch zu vermeiden. Soll ein solcher Heartbeat-Tunnel genutzt werden, dann müssen entsprechende Angaben gemacht werden, die im Folgenden beschrieben werden.

**IPV6\_TUNNEL\_x\_USERID** Diese Variable enthält den Namen des Benutzers, der beim Tunnel-Login erforderlich ist.

Beispiel: `IPV6_TUNNEL_1_USERID='USERID'`

**IPV6\_TUNNEL\_x\_PASSWORD** Diese Variable enthält das Passwort für den oben angegebenen Benutzernamen. Es darf keine Leerzeichen enthalten.

Beispiel: `IPV6_TUNNEL_1_PASSWORD='passwort'`

**IPV6\_TUNNEL\_x\_TUNNELID** Diese Variable enthält den Identifikator des Tunnels.

Beispiel: `IPV6_TUNNEL_1_TUNNELID='TunnelID'`

**IPV6\_TUNNEL\_x\_TIMEOUT** (optional) Diese Variable enthält die Zeitspanne in Sekunden, die beim Tunnelaufbau maximal gewartet wird. Der Standard-Wert ist abhängig vom eingestellten Tunnelanbieter.

Beispiel: `IPV6_TUNNEL_1_TIMEOUT='30'`

### 4.14. ISDN - Kommunikation über aktive und passive ISDN-Karten

fli4l ist vornehmlich zum Einsatz als ISDN- und/oder DSL-Router gedacht. Mit der Einstellung `OPT_ISDN='yes'` wird das ISDN-Paket aktiviert. Voraussetzung ist eine ISDN-Karte, die von fli4l unterstützt wird.

Soll kein ISDN verwendet werden, kann mit der Einstellung `OPT_ISDN='no'` die ISDN-Installation abgeschaltet werden. Dann werden alle in diesem Kapitel folgenden ISDN-Variablen ignoriert.

Standard-Einstellung: `OPT_ISDN='no'`

#### 4.14.1. Herstellen einer ISDN-Verbindung

Das Einwählverhalten von fli4l wird von drei verschiedenen Variablen bestimmt, `DIALMODE`, `ISDN_CIRC_X_ROUTE_X`, `ISDN_CIRC_X_TIMES`. Es wird von [DIALMODE](#) (Seite 96) (in `<config>/base.txt`) bestimmt, ob bei Eintreffen eines Paketes auf einem aktiven Circuit automatisch eine Verbindung aufgebaut werden soll oder nicht. `DIALMODE` kann folgende Werte annehmen:

**auto** Trifft ein Paket auf einem ISDN-Circuit (bzw. dem daraus abgeleiteten ISDN-Interface `ippp*`) ein, wird automatisch eine Verbindung aufgebaut. Ob und wann ein Paket auf einem ISDN-Circuit eintrifft, wird von `ISDN_CIRC_X_ROUTE_X` und `ISDN_CIRC_X_TIMES` bestimmt.

**manual** Im manuellen Modus muß der Verbindungsaufbau über `imond/imonc` angestoßen werden. Wie das geht, steht im Abschnitt über `imonc/imond`.

**off** Es werden keine ISDN-Verbindungen hergestellt.

Auf welchem der konfigurierten Circuits Pakete eintreffen und damit eine Einwahl auslösen können, wird über `ISDN_CIRC_X_ROUTE_X` definiert. Standardmäßig ist es auf `'0.0.0.0/0'`, die sogenannte 'default route' gesetzt. Das heißt, dass alle Pakete, die das lokale Netz verlassen, über diesen Circuit gehen, wenn er aktiv ist. Ob und wann er aktiv ist, wird dabei von `ISDN_CIRC_X_TIMES` bestimmt, da fli4l über die definierten Circuits ein *least cost routing* durchführt (siehe Abschnitt [Least-Cost-Routing - Funktionsweise](#) (Seite 319) in der Dokumentation des Grundpaketes). Möchte man nicht alle Pakete über diesen Circuit leiten, sondern nur Pakete in ein bestimmtes Netz (z.B. Firmennetz), kann man hier ein oder mehrere Netze

angeben. Dann richtet fli4l eine Route über das dem Circuit zugeordnete ISDN-Interface ein, die permanent aktiv ist. Wird nun ein Paket in dieses Netz geschickt, erfolgt automatisch der Verbindungsaufbau.

Wie schon erwähnt, beschreibt `ISDN_CIRC_X_TIMES` neben den Verbindungskosten eines Circuits auch, ob und wann ein Circuit mit einer 'default route' aktiv ist und damit einen Verbindungsaufbau auslösen kann. Das 'wann' spezifiziert man über die Zeit, die ersten beiden Elemente einer time-info (z.B. Mo-Fr:09-18), das 'ob' durch den vierten Parameter `lc-default-route` (y/n). fli4l (bzw. imond) sorgt dann dafür, dass die Pakete, die das lokale Netz verlassen, immer über den zu diesem Zeitpunkt aktiven Circuit gehen und damit ein Herstellen der Verbindung zum Internet-Provider auslösen.

Zusammenfassend kann man also für die Standardanwendungsfälle folgendes sagen:

- Will man einfach nur ins Internet, stellt man `DIALMODE` auf auto, definiert 1-n Circuits, die als erste Route '0.0.0.0/0' haben und deren Zeiten (Zeiten mit `lc-default-route` = y) die gesamte Woche abdecken.

```
ISDN_CIRC_%_ROUTE_N='1'
ISDN_CIRC_%_ROUTE_1='0.0.0.0/0'
ISDN_CIRC_%_TIMES='Mo-Su:00-24:0.0148:Y'
```

- Will man nebenbei noch über eine spezielle Nummer ins Firmennetz, definiert man sich einen Circuit (oder mehrere Circuits) mit Route ungleich '0.0.0.0/0' und hat damit einen permanent aktiven Zugang zum Firmennetz.

```
ISDN_CIRC_%_ROUTE_N='1'
ISDN_CIRC_%_ROUTE_1='network/netmaskbits'
ISDN_CIRC_%_TIMES='Mo-Su:00-24:0.0148:Y'
```

### 4.14.2. ISDN-Karte

Der fli4l-Router unterstützt generell die gleichzeitige Verwendung mehrerer ISDN-Karten. Dies erfordert jedoch, dass alle ISDN-Karten *denselben Treibertyp* benötigen. Der Treibertyp leitet sich aus der Gruppe in der unten stehenden Tabelle ab, in welcher der betreffende Treiber zu finden ist. Es ist also beispielsweise kein Problem, mehrere mISDN-getriebene Adapter oder mehrere HiSax-getriebene Adapter zu verwenden (sofern genügend Ressourcen vorhanden sind), es ist aber nicht möglich, eine mISDN-getriebene und eine HiSax-getriebene Karte zur selben Zeit zu benutzen.

#### **ISDN\_%\_TYPE ISDN\_%\_IO ISDN\_%\_IO0 ISDN\_%\_IO1 ISDN\_%\_MEM ISDN\_%\_IRQ**

Hier sind die technischen Daten für die ISDN-Karte anzugeben.

Die im Beispiel aufgeführten Werte funktionieren für eine TELES 16.3, wenn die Karte auf IO-Adresse 0xd80 eingestellt ist (über Dip-Switches). Bei einer anderen Einstellung der Karte muss der Wert geändert werden.

#### **Häufig gemachter Fehler (Beispiel):**

```
ISDN_1_IO='240' -- richtig wäre: ISDN_1_IO='0x240'
```

#### 4. Pakete

Bei IRQ 12 muss man einen eventuell vorhandenen PS/2-Maus-Anschluss im BIOS abschalten. Sonst besser einen anderen IRQ wählen! „Gute“ sind meist 5, 10 und 11.

ISDN\_%\_TYPE entspricht prinzipiell den Typ-Nummern für den HiSax-Treiber. Ausnahme: nicht-HiSax-Karten wie z.B. AVM-B1. Für diese wurde der Nummernkreis für die Typen erweitert (siehe unten). Die Liste der möglichen HiSax-Typen basiert auf `linux-2.x.y/Documentation/isdn/README.HiSax`.

Typ	Karte	Benötigte Parameter
Dummy Typ-Nummer:		
0	no driver (dummy)	none
Typ-Nummern für Remote-CAPI-Treiber:		
160	AVM Fritz!Box Remote CAPI	ip,port
161	Melware Remote CAPI (rcapi)	ip,port
Typ-Nummern für mISDN-Treiber:		
301	HFC-4S/8S/E1 multiport cards	no parameter
302	HFC-PCI based cards	no parameter
303	HFCS-USB Adapters	no parameter
304	AVM Fritz!Card PCI (v1 and v2) cards	no parameter
305	cards based on Infineon (former Siemens) chips: - Dialogic Diva 2.0 - Dialogic Diva 2.0U - Dialogic Diva 2.01 - Dialogic Diva 2.02 - Sedlbauer Speedwin - HST Saphir3 - Develo (former ELSA) Microlink PCI (Quickstep 1000) - Develo (former ELSA) Quickstep 3000 - Berkom Scitel BRIX Quadro - Dr.Neuhaus (Sagem) Niccy	no parameter
306	NetJet TJ 300 and TJ320 cards	no parameter
307	Sedlbauer Speedfax+ cards	no parameter
308	Winbond 6692 based cards	no parameter

Meine Karte ist eine Teles 16.3 NON-PNP ISA, also ist Type=3.

Für eine ICN-2B-Karte müssen IO und MEM gesetzt werden, zum Beispiel `ISDN_1_IO=0x320`, `ISDN_1_MEM=0xd0000`.

Bei neueren Teles-PCI-Karten muss type=20 (statt 21) verwendet werden. Die Dinger melden sich bei `cat /proc/pci` mit `“tiger”` oder so ähnlich. Sonst kann ich nichts zu diesen Werten beitragen, sorry.

Um die ISDN-Typen 105 bis 114 verwenden zu können, ist es vorher nötig, die passenden Treiberdateien von <http://www.fli4l.de/download/stabile-version/avm-treiber/> herunterzuladen und in das fli4l-Verzeichnis zu entpacken. Da diese Treiber nicht der GPL unterliegen, können sie leider nicht mit dem ISDN Paket mitgeliefert werden.

Für den ISDN-Typ 303 ist es nötig USB Support zu installieren und zu aktivieren. Siehe

dazu [USB - Support für USB-Geräte](#) (Seite 277).

Tips zu den Typ-Nummern bekommt man auch über die i4l-FAQ oder Mailingliste, wenn man wirklich nicht weiß, was da für eine Karte im PC steckt.

Die Kartentypen, die mit „from isapnp setup“ gekennzeichnet sind, müssen mit dem PnP-Tool isapnp initialisiert werden - wenn es sich tatsächlich um eine PnP-Karte handelt. Siehe dazu die Beschreibung im Kapitel [OPT\\_PNP - Installation von isapnp tools](#) (Seite 108).

Der ISDN-Typ 0 wird dann benötigt, wenn man das ISDN-Paket installieren will ohne ISDN-Karte; z.B. um imond verwenden zu können bei einem Netzwerkrouter.

**ISDN\_%\_IP ISDN\_%\_PORT** Für die ISDN-Typen 160 und 161 werden über diese Variablen die IP-Adresse (ISDN\_%\_IP) bzw. der Port (ISDN\_%\_PORT) des Gerätes eingestellt, das eine entfernte CAPI-Schnittstelle anbietet. Die IP-Adresse ist zwingend erforderlich, die Port-Nummer kann hingegen weggelassen werden: Je nach gewähltem Typ wird dann ein Standard-Port eingestellt (Typ 160: 5031, Typ 161: 2662).

Beispiel:

```
ISDN_1_TYPE='160' # AVM Fritz!Box
ISDN_1_IP='192.168.177.1'
```

**ISDN\_DEBUG\_LEVEL** Dieses gibt den Debug-Level für den HiSaX-Treiber an. Der Debug-Level setzt sich dabei durch Addition der folgenden Werte zusammen (Zitat aus der Original-Doku):

Number	Debug-Information
1	Link-level <-> hardware-level communication
2	Top state machine
4	D-Channel Q.931 (call control messages)
8	D-Channel Q.921
16	B-Channel X.75
32	D-Channel l2
64	B-Channel l2
128	D-Channel link state debugging
256	B-Channel link state debugging
512	TEI debug
1024	LOCK debug in callc.c
2048	More debug in callc.c (not for normal use)

Die Standardeinstellung (ISDN\_DEBUG\_LEVEL='31') sollte den meisten reichen.

**ISDN\_VERBOSE\_LEVEL** Hiermit kann man die „Geschwätzigkeit“ des ISDN-Subsystems im fli4l-Kernel einstellen. Jeder Verbose-Level schließt die Level mit niedrigerer Nummer mit ein. Die Verbose-Level sind:

'0'	keine zusätzlichen Informationen
'1'	Es wird protokolliert, was eine ISDN-Verbindung ausgelöst hat
'2' und '3'	Anrufe werden protokolliert
'4' und mehr	Die Datentransferrate wird regelmäßig protokolliert.

Die Meldungen werden über das Kernel-Logging-Interface ausgegeben, erscheinen also bei aktiviertem `OPT_SYSLOGD` (Seite 105) dort.

**Wichtig:** *Sollen Anrufe mit telmond protokolliert werden, diesen Wert nicht kleiner als 2 einstellen, da telmond sonst die Informationen fehlen, um Anrufe zu protokollieren.*

Standardeinstellung: `ISDN_VERBOSE_LEVEL='2'`

**ISDN\_FILTER** Aktiviert den Filtermechanismus des Kerns, um ein ordnungsgemäßes Auflegen nach dem angegebenen Hangup-Timeout zu gewährleisten. Siehe <http://www.fli4l.de/hilfe/howtos/basteleien/hangup-problem-loesen/> für genauere Informationen.

**ISDN\_FILTER\_EXPR** Hier steht der zu nutzende Filter, wenn `ISDN_FILTER` auf 'yes' gesetzt ist.

#### 4.14.3. OPT\_ISDN\_COMP (EXPERIMENTAL)

Mit `OPT_ISDN_COMP='yes'` werden die LZS- und die BSD-Kompression aktiviert. Das Kompressionspaket hat freundlicherweise Arwin Vosselman (E-Mail: [arwin\(at\)xs4all\(dot\)nl](mailto:arwin(at)xs4all(dot)nl)) zusammengestellt. Dieses Zusatzpaket hat Experimental-Status.

Standard-Einstellung: `OPT_ISDN_COMP='no'`

Hier im Einzelnen die erforderlichen Parameter für LZS-Kompression:

**ISDN\_LZS\_DEBUG (EXPERIMENTAL)** Debug-Level-Einstellung:

'0'	keine Debugging Information
'1'	normale Debugging Information
'2'	erweiterte Debugging Information
'3'	schwere Debugging Information (inkl. Dumping der Datenpakete)

Standard-Einstellung: `ISDN_LZS_DEBUG='1'`

Wer bei Problemen mit der Komprimierung noch mehr Debugmeldungen sehen möchte, setzt diese Variable auf '2'.

**ISDN\_LZS\_COMP (EXPERIMENTAL)** Stärke der Kompression (nicht Dekompression!). Bitte erst einmal auf dem Wert '8' stehen lassen. Werte von 0 bis 9 sind möglich.

Grössere Zahlen geben bessere Kompression, 9 erzeugt aber übermässige CPU-Last.

Standard-Einstellung: `ISDN_LZS_COMP='8'`

**ISDN\_LZS\_TWEAK (EXPERIMENTAL)** Auch diese Variable erst einmal auf '7' stehen lassen.

Standard-Einstellung: `ISDN_LZS_TWEAK='7'`

Außer diesen 3 Werten muss noch die Variable `ISDN_CIRC_x_FRAMECOMP` angepasst werden, s. nächstes Kapitel.

#### 4.14.4. ISDN-Circuits

In der fli4l-Konfiguration können mehrere Verbindungen über ISDN definiert werden. Davon sind maximal 2 Verbindungen auch zur gleichen Zeit über eine ISDN-Karte möglich.

Die Definition solcher Verbindungen geschieht über sogenannte Circuits. Dabei wird pro Verbindung ein Circuit verwendet.

In der Beispiel-Datei config.txt sind zwei solcher Circuits definiert:

- Circuit 1: Dialout über Internet-By-Call-Provider Microsoft Network, Sync-PPP
- Circuit 2: Dialin/Dialout zu einem ISDN-Router (das könnte beispielsweise auch fli4l sein) über Raw-IP, z.B. als Zugang zum Firmen-Netz von irgendwo. Bei mir konkret ist das eine Linux-Box mit isdn4linux als "Gegner".

Soll der fli4l-Router lediglich als Internet-Gateway dienen, ist nur ein Circuit notwendig. Ausnahme: Man will die Least-Cost-Router-Features von fli4l nutzen. Dann sind sämtliche erlaubten Circuits für verschiedene Zeitbereiche zu definieren, siehe unten.

**ISDN\_CIRC\_N** Gibt die Anzahl der verwendeten ISDN-Circuits an. Wird fli4l lediglich als ISDN-Anrufmonitor eingesetzt, ist einzustellen:

```
ISDN_CIRC_N='0'
```

Soll der fli4l-Router lediglich als einfaches ISDN-Gateway in das Internet verwendet werden, reicht ein Circuit. Ausnahme: LC-Routing, siehe unten.

**ISDN\_CIRC\_x\_NAME** Hier sollte ein Name für den Circuit vergeben werden - max. 15 Stellen lang. Dieser wird dann im imon-Client `imonc.exe` statt der angewählten Telefonnummer gezeigt. Erlaubte Zeichen sind die Buchstaben 'A' bis 'Z' (Klein- und Großschreibung), die Zahlen '0' bis '9' und der Bindestrich '-', wie z.B.

```
ISDN_CIRC_x_NAME='msn'
```

Der Name kann außerdem im Paketfilter oder bei OpenVPN benutzt werden. Wenn z.B. der Paketfilter einen ISDN Circuit regeln soll, muß ein 'circuit\_' dem Circuit Namen vorangesetzt werden. Heißt ein ISDN Circuit z.B. 'willi', so wird daraus folgendes im Paketfilter:

```
PF_INPUT_3='if:circuit_willi:any prot:udp 192.168.200.226 192.168.200.254:53 ACCEPT'
```

**ISDN\_CIRC\_x\_USEPEERDNS** Hiermit wird festgelegt, ob die vom Internet-Provider bei der Einwahl übergebenen Nameserver für die Dauer der Onlineverbindung in die Konfigurationsdatei des lokalen Nameservers eingetragen werden sollen. Sinnvoll ist die Nutzung dieser Option also nur bei Circuits für Internet-Provider. Inzwischen unterstützen fast alle Provider diese Art der Übergabe.

Nachdem die Nameserver-IP-Adressen übertragen wurden, werden die in der base.txt unter `DNS_FORWARDERS` eingetragenen Nameserver aus der Konfigurationsdatei des lokalen



Nameservers entfernt und die vom Provider vergebenen IP-Adressen als Forwarder eingetragen. Danach wird der lokale Nameserver veranlaßt, seine Konfiguration neu einzulesen. Dabei gehen bis dahin aufgelöste Namen nicht aus dem Nameserver-Cache verloren.

Diese Option bietet den Vorteil, immer mit den am nächsten liegenden Nameservern arbeiten zu können, sofern der Provider die korrekten IP-Adressen übermittelt - dadurch geht die Namensauflösung schneller.

Im Falle eines Ausfalls eines DNS-Servers beim Provider werden in der Regel die übergebenen DNS-Server-Adressen sehr schnell vom Provider korrigiert.

Trotz allem ist vor jeder ersten Einwahl die Angabe eines gültigen Nameservers in *DNS\_FORWARDERS* der base.txt zwingend erforderlich, da sonst die erste Anfrage nicht korrekt aufgelöst werden kann. Außerdem wird beim Beenden der Verbindung die originale Konfiguration des lokalen Nameservers wieder hergestellt.

Standard-Einstellung: `ISDN_CIRC_x_USEPEERDNS='yes'`

**ISDN\_CIRC\_x\_TYPE** `ISDN_CIRC_x_TYPE` gibt den Typ der x-ten IP-Verbindung an. Dabei sind folgende Werte möglich:

'raw' RAW-IP  
'ppp' Sync-PPP

In den meisten Fällen wird PPP verwendet, jedoch ist Raw-IP etwas effizienter, da hier der PPP-Overhead entfällt. Eine Authentifizierung ist zwar bei Raw-IP nicht möglich, es kann jedoch über die Variable `ISDN_CIRC_x_DIALIN` (s.u.) eine Zugangsbeschränkung auf ganz bestimmte ISDN-Nummern (Stichwort "Clip") eingestellt werden. Wird `ISDN_CIRC_x_TYPE` auf 'raw' gestellt wird analog zu den PPP up/down Scripten in `/etc/ppp` ein raw up/down Script ausgeführt.

**ISDN\_CIRC\_x\_BUNDLING** Für die ISDN-Kanalbündelung wird das verbreitete MPPP-Protokoll nach RFC 1717 verwendet. Damit gelten folgende Einschränkungen, die aber in der Praxis meist nicht relevant sind:

- Nur mit PPP-Verbindungen möglich, nicht bei Raw-Circuits
- Kanalbündelung nach neuerer RFC 1990 (MLP) ist nicht möglich

Der 2. Kanal kann entweder mit dem Client imonc manuell hinzugeschaltet werden oder über die Bandbreitenanpassung automatisch aktiviert werden, siehe auch die Beschreibung zu `ISDN_CIRC_x_BANDWIDTH`.

Standard-Einstellung: `ISDN_CIRC_x_BUNDLING='no'`

Vorsicht: bei Verwendung von Kanalbündelung zusammen mit Kompression kann es zu Problemen kommen, siehe auch die Beschreibung zu `ISDN_CIRC_x_FRAMECOMP`.

**ISDN\_CIRC\_x\_BANDWIDTH** Ist die ISDN-Kanalbündelung über `ISDN_CIRC_x_BUNDLING='yes'` aktiviert, kann mit dieser Variablen eine automatische Hinzuschaltung des 2. ISDN-Kanals eingestellt werden. Dabei sind 2 numerische Parameter anzugeben:

1. Schwellenwert in Byte/Sekunde (S)
2. Zeitintervall in Sekunden (Z)

Wird der Schwellenwert S für Z Sekunden überschritten, schaltet der Steuerprozeß imond den 2. Kanal automatisch hinzu. Wird der Schwellenwert S für Z Sekunden unterschritten, wird der 2. Kanal automatisch wieder deaktiviert. Die automatische Bandbreitenanpassung kann mit `ISDN_CIRC_1_BANDWIDTH=""` abgeschaltet werden. Dann ist lediglich eine manuelle Kanalbündelung über den Client imonc möglich.

Beispiele:

- `ISDN_CIRC_1_BANDWIDTH='6144 30'`

Überschreitet die Transferrate den Wert von 6 kibibyte/second für 30 Sekunden, wird der 2. Kanal hinzugeschaltet.

- `ISDN_CIRC_1_BANDWIDTH='0 0'`

Der zweite ISDN-Kanal wird sofort, spätestens 10 Sekunden nach dem Verbindungsaufbau hinzugeschaltet und bleibt solange bestehen, bis die komplette Verbindung beendet wird.

- `ISDN_CIRC_1_BANDWIDTH=""`

Der zweite ISDN-Kanal kann nur manuell hinzugeschaltet werden, Voraussetzung ist jedoch weiterhin, dass `ISDN_CIRC_1_BUNDLING='yes'` eingestellt ist.

- `ISDN_CIRC_1_BANDWIDTH='10000 30'`

Eigentlich sollte hiermit der 2. Kanal nach 30 Sekunden hinzugeschaltet werden, wenn während dieser Zeitspanne 10000 B/s erreicht werden. Dazu wird es aber nicht kommen, da mit ISDN nicht mehr als 8 kB/s erreicht werden können.

Ist `ISDN_CIRC_x_BUNDLING='no'` eingestellt, ist der Wert in der Variablen `ISDN_CIRC_x_BANDWIDTH` belanglos.

Standard-Einstellung: `ISDN_CIRC_x_BANDWIDTH=""`

**ISDN\_CIRC\_x\_LOCAL** In dieser Variablen wird die lokale IP-Adresse auf der ISDN-Seite hinterlegt.

Bei dynamischer Adresszuweisung sollte dieser Wert **leer** sein. Beim Verbindungsaufbau wird dann die IP-Adresse ausgehandelt. In den meisten Fällen vergeben Internet-Provider diese Adresse dynamisch. Soll jedoch eine fest vergebene IP-Adresse verwendet werden, ist diese hier einzutragen. Diese Variable ist optional und muss bei Bedarf in das Konfigfile eingetragen werden.

**ISDN\_CIRC\_x\_REMOTE** In dieser Variablen wird die entfernte IP-Adresse und die zugehörige Netzmaske auf der ISDN-Seite hinterlegt. Dazu muss die CIDR (Classless Inter-Domain Routing) Schreibweise benutzt werden. Details zu [CIDR](#) (Seite 41) ist in der Dokumentation des Baseispaketes bei `IP_NET_x` zu finden.

Bei dynamischer Adresszuweisung sollte dieser Wert **leer** sein. Beim Verbindungsaufbau wird dann die IP-Adresse ausgehandelt. In den meisten Fällen vergeben Internet-Provider diese Adresse dynamisch. Soll jedoch eine fest vergebene IP-Adresse verwendet werden, ist diese hier einzutragen. Diese Variable ist optional und muss bei Bedarf in das Konfigfile eingetragen werden.

Die angegebene Netzmaske wird bei der Configuration des Interfaces nach der Einwahl verwendet. Während dieser Configuration wird auch eine Route zum Host erzeugt, in den

man sich einwählt. Da man diese Route in der Regel nicht braucht, ist es günstig, hier nur eine Route direkt zum Einwahlrechner zu erzeugen. Dazu setzt man die Netzmaske auf /32, indem man hier 32 als Anzahl der gesetzten Bits in der Netzmaske spezifiziert. Für Details siehe [Kapitel: Technische Details zum Dialin](#) (Seite 428).

**ISDN\_CIRC\_x\_MTU ISDN\_CIRC\_x\_MRU** Mit diesen optionalen Variablen können die sog. **MTU** (maximum transmission unit) und die **MRU** (maximum receive unit) eingestellt werden. Optional bedeutet, die Variable muß nicht in der Konfigurationsdatei stehen, sie ist bei Bedarf durch den Benutzer einzufügen!

Normal beträgt die MTU 1500 und die MRU 1524. Diese Einstellung sollte nur in Sonderfällen geändert werden!

**ISDN\_CIRC\_x\_CLAMP\_MSS** Hier sollte man ein yes setzen, wenn man synchrones ppp verwendet (`ISDN_CIRC_x_TYPE='ppp'`) und eines der folgenden Symptome auftritt:

- der Webbrowser verbindet sich mit dem Webserver, aber es wird keine Seite angezeigt und kommt auch keine Fehlermeldung; es passiert einfach nichts mehr,
- das Versenden kleiner E-Mails funktioniert, bei großen gibt es Probleme oder
- ssh funktioniert, scp hängt nach dem initialen Verbindungsaufbau.

Provider, bei denen solche Probleme auftreten, sind z.B. Compuserve und andere Media-ways basierte Zugänge.

Standard-Einstellung: `ISDN_CIRC_x_CLAMP_MSS='no'`

**ISDN\_CIRC\_x\_HEADERCOMP** Mit `ISDN_CIRC_x_HEADERCOMP='yes'` kann die Van-Jacobson-Komprimierung oder Headerkomprimierung eingestellt werden. Nicht alle Provider unterstützen das. Sollte es daher bei eingeschalteter Komprimierung zu Einwahlproblemen kommen, sollte `ISDN_CIRC_x_HEADERCOMP='no'` eingestellt werden.

Standard-Einstellung: `ISDN_CIRC_x_HEADERCOMP='yes'`

**ISDN\_CIRC\_x\_FRAMECOMP (EXPERIMENTAL)** Dieser Parameter wird nur berücksichtigt, wenn `OPT_ISDN_COMP='yes'` eingestellt wird. Er regelt die Frame-Komprimierung.

Folgende Werte sind möglich:

'no'	Keine Frame-Komprimierung
'default'	LZS according RFC1974(std) and BSDCOMP 12
'all'	Negotiate lzs and bsdcomp
'lzs'	Negotiate lzs only
'lzstd'	LZS according RFC1974 Standard Mode ("Sequential Mode")
'lzsext'	LZS according RFC1974 Extended Mode
'bsdcomp'	Negotiate bsdcomp only
'lzstd-mh'	LZS Multihistory according RFC1974 Standard Mode ("Sequential Mode")

Welcher Wert für den jeweiligen Provider verwendet werden kann, muss ausprobiert werden. So weit bekannt geht bei T-Online nur 'lzsext'. Bei den meisten anderen Providern sollte man mit 'default' auskommen.

Vorsicht: Bei verwendung von Kanalbündelung in zusammenhang mit 'lzsext' kann es zu Problemen kommen. Diese Probleme sind, so weit bekannt, Einwahlserverspezifisch und damit meistens Providerspezifisch. Es können aber bei einem Provider auch verschiedene

#### 4. Pakete

Typen Einwahlserver im Einsatz sein, es kann in dem Fall zu Unterschieden zwischen Einwahlknoten kommen.

'lzsstd-mh' ist für Router-zu-Routerbetrieb (r2r) gedacht. Das Verfahren wird von Providern nicht eingesetzt aber bringt bei Verwendung zwischen zwei fli4l-Router erhebliche Verbesserung bei gleichzeitigen Übertragung von mehreren Dateien. Die Headerkompression ist dazu erforderlich und wird deshalb automatisch eingeschaltet.

**ISDN\_CIRC\_x\_REMOTENAME** Diese Variable ist normalerweise lediglich bei der Konfiguration von fli4l als Einwahlrouter relevant. Hier kann ein Name des Remote-Hosts eingetragen werden, muß aber nicht.

Standard-Einstellung: `ISDN_CIRC_x_REMOTENAME=""`

**ISDN\_CIRC\_x\_PASS** Hier sind die Provider-Daten einzutragen. Im Beispiel oben handelt es sich um die Daten des Providers Microsoft Network.

`ISDN_CIRC_x_USER` enthält die Benutzerkennung, `ISDN_CIRC_x_PASS` das Password.

WICHTIG: Für einen T-Online-Zugang ist folgendes zu beachten:

Der Username `AAAAAAAAAAAAATTTTTT#MMMM` setzt sich aus der zwölfstelligen Anschlußkennung, der T-Online-Nummer und der Mitbenutzernummer zusammen. Hinter der T-Online-Nummer muß ein '#' angegeben werden, wenn die Länge der T-Online-Nummer kürzer als 12 Zeichen ist.

Sollte dies in Einzelfällen nicht zum Erfolg führen (offenbar abhängig von der Vermittlungsstelle), muß zusätzlich zwischen der Anschlußkennung und der T-Online-Nummer ein weiteres '#'-Zeichen eingefügt werden.

Ansonsten (T-Online-Nr ist 12stellig) sind keine '#'-Zeichen anzugeben.

Beispiel: `ISDN_CIRC_1_USER='123456#123'`

Bei Raw-IP-Circuits haben diese Variablen keine Bedeutung.

**ISDN\_CIRC\_x\_ROUTE\_N** Die Anzahl der Routen die dieser ISDN Circuit bedient. Wenn dieser Circuit eine Default-Route definiert muss der Eintrag auf '1' gesetzt werden.

**ISDN\_CIRC\_x\_ROUTE\_X** Die Route oder die Routen für diesen Circuit. Für einen Internet-Zugang sollte man hier im ersten Eintrag '0.0.0.0/0' (default route) angeben. Das Format ist immer 'network/netmaskbits'. Eine Hostroute würde z.B. so aussehen: '192.168.199.1/32'. Bei Einwahl in den Firmen- oder Uni-Router ist lediglich das oder die Netze anzugeben, die man dort erreichen will, z.B.

```
ISDN_CIRC_%_ROUTE_N='2'
ISDN_CIRC_%_ROUTE_1='192.168.8.0/24'
ISDN_CIRC_%_ROUTE_2='192.168.9.0/24'
```

Bei mehreren Netzen müssen diese jeweils in einen eigenen Eintrag, also für jede Route muss eine `ISDN_CIRC_x_ROUTE_y=""` Zeile angelegt werden.

Möchte man die LC-Routing-Features von fli4l nutzen, kann \*mehreren\* Circuits eine Default-Route zugewiesen werden. Welcher Circuit dann tatsächlich verwendet wird, wird über `ISDN_CIRC_x_TIMES` eingestellt, siehe unten.

**ISDN\_CIRC\_x\_DIALOUT** ISDN\_CIRC\_x\_DIALOUT gibt die zu wählende Telefonnummer an. Es ist möglich, hier mehrere Nummern anzugeben (falls eine besetzt ist, wird die nächste angewählt) - die Trennung erfolgt dabei durch Leerzeichen. Laut Berichten in der Newsgroup dürfen maximal fünf Nummern angegeben werden.

**ISDN\_CIRC\_x\_DIALIN** Soll der Circuit (auch) zum Einwählen genutzt werden, wird in ISDN\_CIRC\_x\_DIALIN die Rufnummer des Anrufenden eingesetzt - und zwar mit Vorwahl, aber \*ohne\* die erste 0. Bei Anschlüssen hinter Telefonanlagen kann dies anders sein, eventuell müssen dann eine oder sogar zwei führende Nullen angegeben werden.

Soll es mehreren Teilnehmern ermöglicht werden, sich über diesen Circuit einzuwählen, können diese Nummern durch Leerzeichen getrennt angegeben werden. Besser ist es aber, jedem Gegner einen extra Circuit zuzuweisen. Sonst könnte es bei Einwahl von zwei Gegnern zu gleicher Zeit (ist über die 2 ISDN-Kanäle durchaus möglich) auf demselben Circuit zu Kollisionen bzgl. IP-Adressen kommen.

Falls der Anrufende keine Rufnummer überträgt, hier eine '0' setzen. Aber Vorsicht: damit wird jedem eine Anwahl gestattet, der keine Rufnummer überträgt!

Möchte man eine Einwahl unabhängig von der MSN des Anrufenden realisieren, ist als Wert '\*' anzugeben.

In den beiden letzten Fällen ist ein Authentifizierungsverfahren (siehe ISDN\_CIRC\_x\_AUTH) unumgänglich.

**ISDN\_CIRC\_x\_CALLBACK** Einstellung Callbackverfahren, mögliche Werte:

'in'	fli4l wird angerufen und ruft zurück
'out'	fli4l ruft an, hängt jedoch wieder ein und wartet auf Rückruf
'off'	kein Callback
'cbcp'	CallBack Control Protocol
'cbcp0'	CallBack Control Protocol 0
'cbcp3'	CallBack Control Protocol 3
'cbcp6'	CallBack Control Protocol 6

Bei den CallBack Control Protokolle (auch 'Microsoft CallBack' genannt) ist cbcp6 das meist übliche Protokoll.

Standard-Wert: 'off'

**ISDN\_CIRC\_x\_CBNUMBER** Hier kann man für die Protokolle cbcp, cbcp3 und cbcp6 eine Rückrufnummer einsetzen (bei cbcp3 Pflicht).

**ISDN\_CIRC\_x\_CBDELAY** Diese Variable gibt eine Verzögerung in Sekunden an, die bei Callback gewartet werden soll. Je nachdem, in welcher Richtung der Callback erfolgen soll, hat diese Variable eine etwas andere Bedeutung:

- ISDN\_CIRC\_x\_CALLBACK='in':

Wird fli4l angerufen und soll zurückrufen, ist ISDN\_CIRC\_x\_CBDELAY die Wartezeit, bis der Rückruf erfolgen soll. Ein guter Erfahrungswert ist ISDN\_CIRC\_x\_CBDELAY='3'. Je nach "Gegner" kann aber auch ein geringerer Wert funktionieren, welches dann den Verbindungsaufbau beschleunigen kann.

- `ISDN_CIRC_x_CALLBACK='out'`:

In diesem Fall gibt `ISDN_CIRC_x_CBDELAY` die Zeit an, wie lange das “Anklingeln des Gegners” erfolgen soll, bis auf den Rückruf gewartet wird. Auch hier ist `ISDN_CIRC_x_CBDELAY='3'` ein guter Erfahrungswert. Was mir dazu aufgefallen ist: Bei Fernverbindungen muß man bis zu 3 Sekunden “klingeln” lassen, bevor der andere Router überhaupt den Anruf sieht. Bei Ortsverbindungen kann meist dieser Wert kleiner gewählt werden. Im Zweifel: Ausprobieren!

Ist die Variable `ISDN_CIRC_x_CALLBACK='off'` eingestellt, wird `ISDN_CIRC_x_CBDELAY` ignoriert. Auch beim CallBack Control Protocol hat diese Variable keine Bedeutung.

**ISDN\_CIRC\_x\_EAZ** Im Beispiel ist die MSN (hier EAZ genannt) auf 81330 gesetzt. Hier sollte die eigene MSN \*ohne\* Vorwahl eingetragen werden.

Bei Anschlüssen hinter einer Telefonanlage mit Anlagenanschluss ist meistens nur die Durchwahl anzugeben. Ich habe aber auch schon gelesen, dass eine '0' weiterhelfen kann, wenn es Probleme mit der verwendeten Telefonanlage geben sollte.

Dieses Feld kann auch leer sein. Dies soll bei besonders hartnäckigen TK-Anlagen helfen. Um Feedback wird an dieser Stelle gebeten.

**ISDN\_CIRC\_x\_SLAVE\_EAZ** Ist der fli4l-Router am internen S0-Bus einer Telefonanlage angeschlossen und möchte man Kanalbündelung verwenden, ist bei manchen Telefonanlagen die Angabe einer 2. Durchwahlnummer für den Slave-Kanal einzutragen.

Im Normalfall kann diese Variable jedoch leer bleiben.

**ISDN\_CIRC\_x\_DEBUG** Soll `ippdd` zusätzliche Debug-Informationen ausgeben, muss man `ISDN_CIRC_x_DEBUG` auf 'yes' setzen. In diesem Fall schreibt `ippdd` zusätzlichen Informationen über die `syslog`-Schnittstelle.

WICHTIG: Damit diese auch über `syslogd` ausgegeben werden, muss die Variable `OPT_SYSLOGD` (Siehe [OPT\\_SYSLOGD - Programm zum Protokollieren von Systemfehlermeldungen](#) (Seite 105)) ebenso auf 'yes' gesetzt sein.

Weil manche Meldungen über `klog` ausgegeben werden sollte man beim Debuggen von ISDN auch `OPT_KLOGD` (Siehe [OPT\\_KLOGD - Kernel-Message-Logger](#) (Seite 107)) auf 'yes' setzen.

Bei Raw-IP-Circuits hat `ISDN_CIRC_x_DEBUG` keine Bedeutung.

**ISDN\_CIRC\_x\_AUTH** Wird dieser Circuit auch zum Einwählen verwendet und soll eine Authentifizierung über PAP oder CHAP vom einwählenden “Gegner” gefordert werden, ist `ISDN_CIRC_x_AUTH` auf 'pap' oder 'chap' zu setzen - und \*nur\* dann. Anderenfalls immer leer lassen!

Grund: Ein angewählter Internet-Provider wird es immer ablehnen, sich selbst auszuweisen! Ausnahmen bestätigen die Regel, wie ich erst kürzlich in der i4l-Mailingliste las ...

Als Benutzername und Passwort werden die Einträge von `ISDN_CIRC_x_USER` und `ISDN_CIRC_x_PASS` benutzt.

Bei Raw-IP-Circuits hat diese Variable keine Bedeutung.

**ISDN\_CIRC\_x\_HUP\_TIMEOUT** Mit der Variablen ISDN\_CIRC\_x\_HUP\_TIMEOUT wird die Zeit gesteuert, nach der der fli4l-Rechner die Verbindung zum Provider beenden soll, wenn nichts mehr über die Leitung geht. Im Beispiel wird die Verbindung nach 40 Sekunden Idle-Time abgebaut, um Geld zu sparen. Bei einem erneuten Zugriff in's Netz wird die Verbindung in Sekundenschnelle wieder aufgebaut. Sinnvoll bei Providern, die sekunden-genau abrechnen!

Man sollte zumindest in der Testphase das automatische Wählen/Einhängen des fli4l-Routers beobachten (entweder auf der Console oder im imon-Client für Windows). Nicht, dass durch eine fehlerhafte Konfiguration der ISDN-Anschluss zur Standleitung wird.

Wird der Wert auf '0' gestellt, wird keine Idle-Zeit mehr berücksichtigt, d.h. fli4l hängt von sich aus die Leitung nicht mehr ein. Bitte mit Vorsicht anwenden.

**ISDN\_CIRC\_x\_CHARGEINT** Charge-Interval: Hier ist der Zeittakt in Sekunden anzugeben. Dieser wird dann für die Kosten-Berechnung verwendet.

Die meisten Provider rechnen minutengenau ab. In diesem Fall ist der Wert '60' richtig. Compuserve verwendet einen 3-Minuten-Takt (Stand Juni 2000), also ISDN\_CIRC\_x\_CHARGEINT='180'. Bei Providern mit sekundengenauer Abrechnung (z.B. Planet-Interkom) setzt man besser ISDN\_CIRC\_x\_CHARGEINT auf '1'.

Erweiterung für ISDN\_CIRC\_x\_CHARGEINT >= 60 Sekunden:

Wurde ISDN\_CIRC\_x\_HUP\_TIMEOUT Sekunden lang kein Traffic bemerkt, wird ca. 2 Sekunden vor Ablauf des Taktes eingehängt. Die vom Provider berechnete Zeit wird also fast komplett ausgenutzt. Ein wirklich tolles Feature von isdn4linux!

Bei sekundengenau abgerechneten Verbindungen hat das natürlich keinen Sinn - daher gilt diese Regelung erst ab Zeittakten von 60 Sekunden.

**ISDN\_CIRC\_x\_TIMES** Hier werden die Zeiten angegeben, wann dieser Circuit aktiviert werden soll und wann er wieviel kostet. Dadurch wird es möglich, zu verschiedenen Zeiten verschiedene Circuits mit Default-Routen zu verwenden (Least-Cost-Routing). Dabei kontrolliert der Daemon imond die Routen-Zuweisung.

Aufbau der Variablen:

```
ISDN_CIRC_x_TIMES='times-1-info [times-2-info] ...'
```

Jedes Feld times-?-info besteht aus 4 Unterfeldern - durch Doppelpunkt (':') getrennt.

1. Feld: W1-W2

Wochentag-Zeitraum, z.B. Mo-Fr oder Sa-Su usw. Schreibweise in Englisch oder deutsch möglich. Soll ein einzelner Wochentag eingetragen werden, ist zu W1-W1 schreiben, also z.B. Su-Su.

2. Feld: hh-hh

Stunden-Bereich, z.B. 09-18 oder auch 18-09. 18-09 ist gleichbedeutend mit 18-24 plus 00-09. 00-24 meint den ganzen Tag.

3. Feld: Charge

Hier werden in Euro-Werten die Kosten pro Minute angegeben, z.B. 0.032 für 3.2 Cent pro Minute. Diese werden unter Berücksichtigung der Taktzeit umgerechnet für die tatsächlich anfallenden Kosten, welche dann im imon-Client angezeigt werden.

#### 4. Feld: LC-Default-Route

Der Inhalt kann Y oder N sein. Dabei bedeutet:

- Y: Der angegebene Zeitbereich wird beim LC-Routing als Default-Route verwendet. Wichtig: In diesem Fall muss auch `ISDN_CIRC_x_ROUTE='0.0.0.0/0'` sein!
- N: Der angegebene Zeitbereich dient nur zum Berechnen von Kosten, er wird beim automatischen LC-Routing jedoch nicht weiter verwendet.

Beispiel:

```
ISDN_CIRC_1_TIMES='Mo-Fr:09-18:0.049:N Mo-Fr:18-09:0.044:Y Sa-Su:00-24:0.044:Y'  
ISDN_CIRC_2_TIMES='Mo-Fr:09-18:0.019:Y Mo-Fr:18-09:0.044:N Sa-Su:00-24:0.044:N'
```

Die Bedeutung ist dabei wie folgt: Circuit 1 (Provider Planet-Interkom) soll abends an Werktagen und komplett am Wochenende verwendet werden, jedoch tagsüber an Werktagen der Circuit 2 (Provider Compuserve).

**Wichtig:** *Die bei ISDN\_CIRC\_x\_TIMES angegebenen Zeiten muessen die ganze Woche abdecken. Ist das nicht der Fall, kann keine gültige Konfiguration erzeugt werden.*

*Wenn die Zeitbereiche aller LC-Default-Route-Circuits ("Y") zusammengenommen nicht die komplette Woche beinhalten, gibt's zu diesen Lückenzeiten keine Default-Route. Damit ist dann Surfen im Internet zu diesen Zeiten ausgeschlossen!*

Beispiel:

```
ISDN_CIRC_1_TIMES='Sa-Su:00-24:0.044:Y Mo-Fr:09-18:0.049:N Mo-Fr:18-09:0.044:N'  
ISDN_CIRC_2_TIMES='Sa-Su:00-24:0.044:N Mo-Fr:09-18:0.019:Y Mo-Fr:18-09:0.044:N'
```

Hier wurde für die Werktage von 18-09 Uhr "N" gesetzt. Zu diesen Zeiten gibt es keine Route in's Internet: Surfen verboten!

Noch ein ganz einfaches Beispiel:

```
ISDN_CIRC_1_TIMES='Mo-Su:00-24:0.0:Y'
```

für diejenigen, die eine Flatrate nutzen.

Und noch eine letzte Bemerkung zum LC-Routing:

Deutsche Feiertage werden wie Sonntage behandelt.

#### 4.14.5. OPT\_TELMOND - telmond-Konfiguration

Mit OPT\_TELMOND kann man einstellen, ob der telmond-Server aktiviert werden soll. Dieser horcht auf eingehende Telefonanrufe und teilt über TCP-Port 5001 die anrufende und die angerufene Telefonnummer mit. Diese Information kann vom Windows- und Unix/Linux-Client imonc abgefragt und angezeigt werden (s.a. Kapitel "Client-/Server-Schnittstelle imond").

Zwingende Voraussetzung ist hierfür die Installation einer ISDN-Karte und die Konfiguration von OPT\_ISDN und den dazugehörigen Konfigurations-Variablen.

Im laufenden Betrieb kann die korrekte Funktion von telmond unter Linux/Unix/Windows überprüft werden mit:



```
telnet fli4l 5001
```

Dann sollte der letzte Anruf gezeigt und anschließend die telnet-Verbindung sofort wieder geschlossen werden.

Der Port 5001 ist nur vom LAN aus erreichbar. Standardmäßig wird ein Zugriff von außen über die Firewall-Konfiguration abgeblockt. Möchte man jedoch auch den Zugriff innerhalb des LANs anders regeln, kann dies über die weitere telmond-Konfigurationsvariablen eingestellt werden, siehe unten.

Standard-Einstellung: `START_TELMOND='yes'`

**TELMOND\_PORT** TCP/IP-Port, auf dem telmond auf Verbindungen horcht. Der Standardwert '5001' sollte nur in Ausnahmefällen geändert werden.

**TELMOND\_LOG** Bei `TELMOND_LOG='yes'` werden sämtliche einkommenden Telefonanrufe in der Datei `/var/log/telmond.log` gespeichert. Der Inhalt der Datei kann mit dem imond-Client `imonc` unter Unix/Linux und Windows abgefragt werden.

Abweichende Pfade bzw. nach Clients aufgeteilte Log-Dateien können weiter unten konfiguriert werden.

Standard-Einstellung: `TELMOND_LOG='no'`

**TELMOND\_LOGDIR** Ist das Protokollieren eingeschaltet, kann über `TELMOND_LOGDIR` ein alternatives Verzeichnis statt `/var/log` angegeben werden, z.B. `'/boot'`. Dann wird die LOG-Datei `telmond.log` auf dem Bootmedium angelegt. Dazu muß dann das Bootmedium auch Read/Write "gemounted" sein. Wird hier 'auto' angegeben, befindet sich das Logfile je nach Konfiguration unter `/boot/persistent/isdn` oder an einem anderen durch `FLI4L_UUID` bestimmten Pfad. Wenn `/boot` nicht Read/Write gemountet ist, wird das File in `/var/run` angelegt.

**TELMOND\_MSN\_N** Sollen bestimmte Anrufe nur auf einigen PC-Clients im `imonc` sichtbar werden, kann ein Filter eingestellt werden, mit dem Anrufe auf spezielle MSNs nur für diese PC-Clients protokolliert werden.

Ist so etwas notwendig, z.B. in einer WG, wird die Variable `TELMOND_MSN_N` auf die Anzahl der MSN-Filter eingestellt.

Standard-Einstellung: `TELMOND_MSN_N='0'`

**TELMOND\_MSN\_x** Für jeden MSN-Filter ist eine Liste von IP-Adressen anzugeben, für welche die Anrufe auf eingetragene MSN sichtbar werden sollen.

Die Variable `TELMOND_MSN_N` bestimmt die Anzahl solcher Konfigurationen, siehe oben.

Der Aufbau der Variablen ist:

```
TELMOND_MSN_x='MSN IP-ADDR-1 IP-ADDR-2 ...'
```

Ein einfaches Beispiel:

```
TELMOND_MSN_1='123456789 192.168.6.2'
```

Soll ein Anruf auf eine bestimmte MSN auf mehreren Rechnern sichtbar werden, z.B. Fax, sind die IP-Adressen der Rechner hintereinander anzugeben, z.B.

```
TELMOND_MSN_1='123456789 192.168.6.2 192.168.6.3'
```

**TELMOND\_CMD\_N** Sobald ein Telefonanruf (Voice) auf einer bestimmten MSN hereinkommt, können optional bestimmte Kommandos auf dem fli4l-Router ausgeführt werden. Mit TELMOND\_CMD\_N gibt man die Anzahl der konfigurierten Kommandos an.

**TELMOND\_CMD\_x** Mit TELMOND\_CMD\_1 bis TELMOND\_CMD\_n können Kommandos angegeben werden, welche ausgeführt werden, wenn ein Telefonanruf eintrifft.

Die Variable TELMOND\_CMD\_N bestimmt die Anzahl solcher Kommandos, siehe oben.

Die Variable hat folgenden Aufbau:

```
MSN CALLER-NUMBER  COMMAND ...
```

Dabei ist die MSN ohne Vorwahl einzutragen. Als CALLER-NUMBER gibt man die komplette Telefonnummer - also mit Vorwahl - an. Schreibt man als Wert für CALLER-NUMBER ein einfaches Sternchen (\*), wird von telmond die Telefonnummer des Anrufers nicht ausgewertet.

Hier ein Beispiel:

```
TELMOND_CMD_1='1234567 0987654321 sleep 5; imonc dial'
TELMOND_CMD_2='1234568 * switch-on-coffee-machine'
```

Im ersten Fall wird die Kommandofolge “sleep 5; imonc dial” durchgeführt, wenn der Anrufer mit der Telefonnummer 0987654321 die MSN 1234567 anruft. Tatsächlich werden hier 2 Kommandos ausgeführt. Zunächst wird 5 Sekunden gewartet, damit der ISDN-Kanal wieder frei wird, auf dem der Anruf hereinkam. Anschließend wird der fli4l-Client imonc mit dem Argument “dial” gestartet. imonc gibt dieses Kommando 1:1 an den Server imond weiter, welcher dann auf dem Default-Circuit eine Netzverbindung herstellt, z.B. ins Internet. Welche Kommandos das imonc-Client-Programm an den Server imond weitergeben kann, ist im Kapitel “Client-/Server-Schnittstelle imond” erklärt. Damit diese Einstellung funktioniert, muss OPT\_IMONC aus dem Paket “tools” installiert sein.

Das zweite Kommando “switch-on-coffee-machine” wird ausgeführt, wenn ein Anruf auf der MSN 1234568 hereinkommt, unabhängig, woher der Anruf kam. Natürlich gibt es das Kommando “switch-on-coffee-machine” (noch) nicht für fli4l!

Beim Aufruf der Kommandos können folgende Platzhalter verwendet werden:

%d	date	Datum
%t	time	Uhrzeit
%p	phone	Telefonnummer des Anrufers
%m	msn	Eigene MSN
%%	percent	das Prozentzeichen selbst

Diese Daten können dann von den aufgerufenen Programmen weiter verwendet werden, z.B. zum Verschicken per E-Mail.

**TELMOND\_CAPI\_CTRL\_N** Wenn Sie einen CAPI-fähigen ISDN-Adapter oder eine Remote-CAPI (Typ 160 oder 161) verwenden, kann es sein, dass Sie die CAPI-Controller, an denen telmond auf Anrufe horcht, genauer konfigurieren wollen. Beispielsweise bietet die Fritz!Box Zugriff auf teilweise bis zu fünf verschiedene Controller an, von denen manche sich nicht unterscheiden (siehe hierzu die Informationen unter [http://www.wehavemorefun.de/fritzbox/CAPI-over-TCP#Virtuelle\\_Controller](http://www.wehavemorefun.de/fritzbox/CAPI-over-TCP#Virtuelle_Controller)). Um die zu verwendenden Controller einzuschränken, können Sie hier die Anzahl der zu nutzenden Controller angeben. In der nachfolgenden Array-Variable TELMOND\_CAPI\_CTRL\_% können Sie dann angeben, welche Controller genutzt werden sollen.

Wenn Sie diese Variable nicht nutzen, horcht telmond auf *allen* verfügbaren CAPI-Controllern.

**TELMOND\_CAPI\_CTRL\_x** Wenn sie TELMOND\_CAPI\_CTRL\_N ungleich Null gesetzt haben, müssen Sie in den Einträgen dieses Arrays die Indizes der CAPI-Controller angeben, an denen telmond auf eingehende Anrufe horchen soll.

Beispiel für die Remote-CAPI einer Fritz!Box mit "echtem" ISDN-Anschluss:

```
TELMOND_CAPI_CTRL_N='2'
TELMOND_CAPI_CTRL_1='1' # horche auf eingehende ISDN-Anrufe
TELMOND_CAPI_CTRL_2='3' # horche auf Anrufe auf dem internen S0-Bus
```

Beispiel für die Remote-CAPI einer Fritz!Box mit analogem Anschluss und SIP-Weiterleitung:

```
TELMOND_CAPI_CTRL_N='2'
TELMOND_CAPI_CTRL_1='4' # horche auf eingehende analoge Anrufe
TELMOND_CAPI_CTRL_2='5' # horche auf eingehende SIP-Anrufe
```

### 4.14.6. OPT\_RCAPID - Remote CAPI Dämon

Dieses OPT konfiguriert auf dem fli4l-Router das Programm rcapid, das Zugriff auf die ISDN-CAPI-Schnittstelle des Routers übers Netzwerk anbietet. Geeignete Anwendungen können somit die ISDN-Karte des Routers übers Netzwerk so nutzen, als ob sie lokal zur Verfügung stünde. Die Funktionalität ähnelt somit dem Paket "mtgcapri". Der Unterschied besteht jedoch darin, dass "mtgcapri" nur Windows-Systeme als Klienten unterstützt, während die Netzwerk-Schnittstelle des rcapid nach Kenntnis des Autors zur Zeit nur Linux-Systeme nutzen können. Insofern ergänzen sich in gemischten Umgebungen mit Windows- und Linux-Systemen beide Pakete ideal.

#### Konfiguration des Routers

**OPT\_RCAPID** Diese Variable aktiviert das Anbieten der auf dem Router verfügbaren ISDN-CAPI für entfernte Klienten. Mögliche Werte sind "yes" und "no". Wird diese Variable auf "yes" gesetzt, wird der Internet-Dämon inetd so konfiguriert, dass auf Anfragen am rcapid-Port 6000 der rcapid-Dämon gestartet wird (der Port kann mit Hilfe der Variablen RCAPID\_PORT geändert werden).

Beispiel: OPT\_RCAPID='yes'

**RCAPID\_PORT** Diese Variable enthält den TCP-Port, den der rcapid-Dämon benutzen soll.

Standard-Einstellung: RCAPID\_PORT='6000'

## Konfiguration der Linux-Klienten

Um auf einem Linux-Rechner die entfernte CAPI-Schnittstelle nutzen zu können, muss die modulare libcapi20-Bibliothek verwendet werden. Aktuelle Linux-Distributionen installieren bereits eine solche CAPI-Bibliothek (z.B. Debian Wheezy). Falls nicht, können die Quellen von [http://ftp.de.debian.org/debian/pool/main/i/isdnutils/isdnutils\\_3.25+dfsg1.orig.tar.bz2](http://ftp.de.debian.org/debian/pool/main/i/isdnutils/isdnutils_3.25+dfsg1.orig.tar.bz2) heruntergeladen werden; nach dem Auspacken und dem Wechsel ins Verzeichnis “capi20” kann die CAPI-Bibliothek mit dem üblichen Dreierschritt “./configure”, “make” und “sudo make install” übersetzt und installiert werden. Ist die Bibliothek erst einmal installiert, muss man nur noch in der Konfigurationsdatei `/etc/capi20.conf` vermerken, auf welchem Rechner das rcapid-Programm läuft. Ist der Router beispielsweise unter dem Namen “fli4l” erreichbar, sieht die Konfigurationsdatei folgendermaßen aus:

```
REMOTE fli4l 6000
```

Das war's! Ist auf dem Linux-Klienten das Programm “capiinfo” installiert (Teil des capi4k-utils-Pakets vieler Distributionen), dann kann man sofort die entfernte CAPI-Schnittstelle testen:

```
kristov@peacock ~ $ capiinfo
Number of Controllers : 1
Controller 1:
Manufacturer: AVM Berlin
CAPI Version: 1073741824.1229996355
Manufacturer Version: 2.2-00 (808333856.1377840928)
Serial Number: 0004711
BChannels: 2
[...]
```

Unter “Number of Controllers” wird die Anzahl der ISDN-Karten vermerkt, die auf dem Klienten nutzbar sind. Steht hier “0”, dann funktioniert zwar die Verbindung zum rcapid-Programm, aber auf dem Router wird/werden die ISDN-Karte(n) nicht erkannt. Funktioniert die Verbindung zum rcapid-Programm gar nicht (z.B. weil `OPT_RCAPID` auf “no” steht), dann erscheint die Fehlermeldung “capi not installed - Connection refused (111)”. In diesem Fall sollte man die Konfiguration noch einmal überprüfen.

## 4.15. OpenVPN - VPN-Support

Ab Version 2.1.5 ist das OpenVPN Paket fester Bestandteil von fli4l.

**Wichtig:** Für die Nutzung von OpenVPN über das Internet, ist in jedem Fall eine Flatrate oder eine volumenbasierte Abrechnung notwendig! Wenn der fli4l-Router permanent eingeschaltet bleibt, wird die Verbindung nicht getrennt, da permanent Daten (wenn auch nur ein paar Bytes alle paar Sekunden) übertragen werden. Mit der Nutzung eines der VPN Pakete und der Verwendung eines VPN Tunnel über das Internet, legt der fli4l-Router nicht mehr auf und es entstehen hohe Kosten, wenn keine Flatrate oder ein volumenbasiertes Abrechnungsmodell benutzt wird! Gleiches gilt natürlich für eine ISDN Wählleitung.

Neben OpenVPN gibt es in der opt-Datenbank <http://www.fli4l.de/download/zusatzpakete/> noch das VPN Paket `OPT_PoPToP`.

Die Entscheidung für eine VPN Lösung hängt in erster Linie von der Sicherheit und der Funktion der eingesetzten Lösung ab. Aussagen zur Sicherheit der hier angebotenen VPN Lösungen gibt das fli4l Team bewusst nicht ab, verweist dafür auf folgende Webseiten und Berichte:

Linux-Magazin Ausgabe Januar 2004

<http://diswww.mit.edu/bloom-picayune/crypto/14238>

<http://sites.inka.de/bigred/archive/cipe-1/2003-09/msg00263.html>

Zur Funktionalität kann das fli4l Team aber eine klare Aussage treffen. In diesem Punkt ist OpenVPN der klare Gewinner gegenüber CIPE und poptop. OpenVPN unterstützt neben einem Tunnel- und Bridgemodus auch Datenkompression und läuft im Gegensatz zu CIPE wesentlich stabiler auf dem fli4l-Router. Außerdem gibt es für OpenVPN auch eine Windows Version, die ab Windows 2000 eingesetzt werden kann. Einziger Nachteil von OpenVPN ist seine Größe im opt-Archiv gegenüber CIPE und die fehlende OpenVPN Unterstützung für fli4l Version 2.0.x.

#### 4.15.1. OpenVPN - Einführendes Beispiel

Um den Einstieg in die Konfiguration zu erleichtern, vorab ein kleines Beispiel. Es sollen zwei Netze, die beide einen fli4l-Router einsetzen, über das Internet verbunden werden. Dazu wird von OpenVPN auf den zwei fli4l-Router ein verschlüsselter Tunnel eingerichtet, durch den die Computer aus den entfernten Netzen miteinander kommunizieren können. Dabei spielen die im Bild 4.1 gezeigten Konfigurationsvariablen eine Rolle.

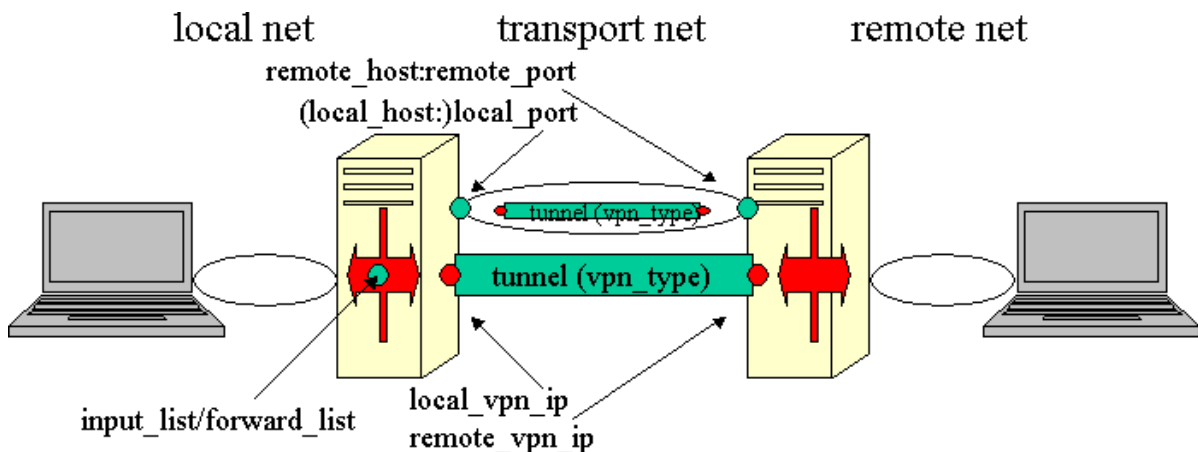


Abbildung 4.1.: VPN-Konfigurationsbeispiel — Tunnel zwischen zwei Routern

**local net, remote net** repräsentieren die beiden Netze, die über den Tunnel miteinander verbunden werden sollen. Die beiden zu verbindenden Netze müssen in unterschiedlichen TCP/IP Netzen sein und dürfen sich in ihren Netzmasken auch nicht überschneiden. Die Einstellungen von `IP_NET_x` (Seite 41) in der jeweiligen `base.txt` Konfigurationsdateien dürfen also nicht gleich sein. Es ist also mit einem VPN Tunnel nicht möglich zwei Netze miteinander zu verbinden, die beide das IP Netz 192.168.6.0/24 benutzen.

**transport net** das Transport Netzwerk besteht aus zwei Elementen:

- der Verbindung zwischen zwei OpenVPN-Daemons, beschrieben durch `remote_host:remote_port` und `(local_host):local_port`. Das entspricht den

OpenVPN Einstellungen OPENVPN\_x\_REMOTE\_HOST, OPENVPN\_x\_REMOTE\_PORT, OPENVPN\_x\_LOCAL\_HOST und OPENVPN\_x\_LOCAL\_PORT.

- und dem Tunnel, über den die Verbindung zwischen den OpenVPN-Daemons etabliert wird, beschrieben durch [local\\_vpn\\_ip](#)/[remote\\_vpn\\_ip](#). Dies entspricht dann wieder OPENVPN\_x\_LOCAL\_VPN\_IP und OPENVPN\_x\_REMOTE\_VPN\_IP. Die beiden VPN IP-Adressen dürfen sich dabei in keinem anderen, den beiden Routern bekannten Netzen liegen.

**input\_list, forward\_list** Pakete, die über den Tunnel gehen sollen, müssen zuerst durch den Paketfilter. Dieser erlaubt standardmäßig nur ICMP-Nachrichten (z. B. ping), die man zum Testen des Tunnels verwenden kann. Alles andere muß erst explizit erlaubt werden, im einfachsten Falle durch

```
OPENVPN_x_PF_INPUT_POLICY='ACCEPT'  
OPENVPN_x_PF_FORWARD_POLICY='ACCEPT'
```

**Bitte denken Sie daran, dass das komplette „Freigeben“ einer VPN Verbindung sicherheitstechnisch sehr bedenklich ist. Benutzen Sie lieber die tmpl: Syntax des Paketfilters, um nur gezielt die Dienste freizugeben, die Sie auch benötigen.**

Mehr Einstellungen sind für einen einfachen VPN Tunnel nicht notwendig. Alle weiteren Einstellmöglichkeiten behandeln erweiterte Funktionen oder sind für spezielle Anwendungsfälle gedacht. Sie sollten mit diesen erweiterten Einstellungen erst dann arbeiten, weil der VPN Tunnel mit den minimalen Einstellungen erfolgreich aufgebaut werden kann.

#### 4.15.2. OpenVPN - Konfiguration

Da OpenVPN ziemlich komplex ist, beginnen wir mit der Erklärung der zwingend notwendigen Angaben für jede VPN Verbindung. Erst wenn der fli4l-Router mit diesen Einstellungen eine Verbindung aufgebaut hat, sollten Sie sich daran wagen die erweiterten Konfigurationsmöglichkeiten von OpenVPN zu nutzen.

**OPT\_OPENVPN** Default: OPT\_OPENVPN='no'

Mit 'yes' wird das OpenVPN Paket aktiviert. Die Einstellung 'no' deaktiviert das OpenVPN Paket komplett.

**OPENVPN\_N** Default: OPENVPN\_N='0'

Wieviele OpenVPN Konfigurationen sind in der Konfigurationsdatei aktiv?

**OPENVPN\_x\_REMOTE\_HOST** Default: OPENVPN\_x\_REMOTE\_HOST=""

Die IP-Adresse oder eine DNS-Adresse der OpenVPN Gegenstelle. Bei einem [Roadwarrior](#) (Seite 222) muss diese Zeile komplett fehlen. Wird diese Einstellung weggelassen, wartet OpenVPN auf einen Verbindungsaufbau und versucht nicht selbstständig die Verbindung aufzubauen.

**OPENVPN\_x\_REMOTE\_HOST\_N** Default: `OPENVPN_x_REMOTE_HOST_N='0'`

Bei der Benutzung von dynamischen DNS Diensten passiert es leider ab und an, dass ein Dienst nicht 100% zuverlässig funktioniert. Daher macht es in diesen Fällen Sinn, einfach zwei oder mehr DynDNS Dienste zu benutzen und seine aktuelle IP-Adresse bei allen Diensten gleichzeitig zu registrieren. Damit OpenVPN in diesem Fall auch alle DynDNS Namen durchgehen kann, muss hier noch die Liste der *zusätzlichen* DNS Namen eingegeben werden. Zusammen mit `OPENVPN_x_REMOTE_HOST` ergibt sich dann die Liste der DynDNS Adressen, die OpenVPN in zufälliger Reihenfolge zu kontaktieren versucht. Der Eintrag `OPENVPN_x_REMOTE_HOST` muss also weiterhin vorhanden sein!

**OPENVPN\_x\_REMOTE\_HOST\_x** Default: `OPENVPN_x_REMOTE_HOST_x=""`

Es gilt die gleiche Beschreibung wie unter [OPENVPN\\_x\\_REMOTE\\_HOST](#) (Seite 198).

**OPENVPN\_x\_REMOTE\_PORT** Default: `OPENVPN_x_REMOTE_PORT=""`

Jede OpenVPN Verbindung braucht eine auf dem fli4l-Router bisher nicht benutzte Port-Adresse. Es empfiehlt sich, einen Port oberhalb von 10000 zu nehmen, da dort normalerweise keine häufig benutzten Ports liegen. Wenn Sie eine Verbindung für eine Gegenstelle bereitstellen wollen, die eine wechselnde IP-Adresse hat und über keine DynDNS Adresse verfügt, lassen Sie diesen Eintrag genau wie `OPENVPN_x_REMOTE_HOST` komplett weg.

**OPENVPN\_x\_LOCAL\_HOST** Default: `OPENVPN_x_LOCAL_HOST=""`

Gibt an, an welche IP-Adresse OpenVPN gebunden werden soll. Bei Verbindungen über das Internet sollte dieser Eintrag leer bleiben oder komplett weggelassen werden. Wird hier eine IP-Adresse angegeben, horcht OpenVPN nur auf dieser IP-Adresse auf eingehende Verbindungsanfragen. Wenn Sie eine WLAN Verbindung absichern wollen, sollten Sie hier die IP-Adresse der WLAN Karte vom fli4l-Router eintragen.

**OPENVPN\_x\_LOCAL\_PORT** Default: `OPENVPN_x_LOCAL_PORT=""`

Gibt die Portnummer an, auf der der lokale OpenVPN Daemon horcht. Für jede OpenVPN Einstellung benötigen Sie einen dafür reservierten Port, d.h. dieser Port kann nur von dieser einer OpenVPN Verbindung benutzt werden und darf auch von keiner anderen Software auf dem fli4l-Router benutzt werden. Die Einstellungen `OPENVPN_x_REMOTE_PORT` und `OPENVPN_x_LOCAL_PORT` jeder OpenVPN Verbindung müssen zusammenpassen! Wenn Sie auf einer Seite des Tunnel `OPENVPN_x_REMOTE_PORT='10111'` setzen *muss* die andere zwingend auf `OPENVPN_x_LOCAL_PORT='10111'` gesetzt werden.

Nochmal: Es ist sehr wichtig, diese Einstellungen auf die jeweilige OpenVPN Gegenstelle anzupassen, sonst ist eine Verbindung zwischen den OpenVPN Partnern nicht möglich.

Damit OpenVPN auf eingehende Verbindungen horchen kann, öffnet OpenVPN selbstständig die Ports im Paketfilter, die unter `OPENVPN_x_LOCAL_PORT` angegeben werden. Wenn dies nicht gewünscht wird, können Sie dies unter [OPENVPN\\_DEFAULT\\_OPEN\\_OVPNPORT](#) (Seite 208) anpassen. Es ist *nicht* notwendig den Eintrag `OPENVPN_DEFAULT_OPEN_OVPNPORT='yes'` zu setzen, da das die Standardeinstellung ist!

Es ist nicht möglich OpenVPN auf Ports kleiner als 1025 horchen zu lassen. Wenn Sie z.B. einen OpenVPN als tcp4- oder tcp6-server auf Port 443 (der https Port) konfigurieren wollen, müssen Sie den Port 443 per Paketfilter an einen Port über 1024 weiterleiten.

Wenn Sie z.B. den OpenVPN auf Port 5555 horchen lassen und den Port 443 weiterleiten wollen, muss folgendes in die `PF_PREROUTING` eingetragen werden.

```
PF_PREROUTING_5='tmpl:https dynamic REDIRECT:5555'
```

#### **OPENVPN\_x\_SECRET** Default: `OPENVPN_x_SECRET=""`

OpenVPN benötigt zum Verschlüsseln der OpenVPN Verbindung ein sogenanntes Keyfile. Dieses Keyfile kann unter Windows oder Linux direkt mit OpenVPN erzeugt werden. Für Anfänger bietet es sich an, die Windows Software von OpenVPN zu installieren oder die OpenVPN WebGUI zu benutzen. Wenn Sie OpenVPN unter Windows nicht einsetzen wollen, sondern nur die für OpenVPN benötigten Keyfiles erstellen wollen, reicht es, die Punkte *OpenVPN User-Space Components*, *OpenSSL DDLs*, *OpenSSL Utilities*, *Add OpenVPN to PATH* und *Add Shortcuts to OpenVPN* zu installieren. Mit dem Menüpunkt *Generate a static OpenVPN key*, den Sie im Startmenü unter OpenVPN finden, können dann die benötigten Keydateien erzeugt werden. Nach dem Aufruf des Menüpunktes kommt die Meldung „Randomly generated 2048 bit key written to C:/Programme/OpenVPN/config/key.txt“. Die erstellte `key.txt` Datei ist das benötigte Keyfile. Kopieren Sie diese Datei einfach in das Verzeichnis `<config>/etc/openvpn` und benennen Sie die `key.txt` entsprechend um, so dass der Dateiname aussagekräftig wird. Sie können ein Keyfile auch automatisch vom fli4l-Router erstellen lassen, wenn Sie `OPENVPN_CREATE_SECRET` auf 'yes' stellen und den fli4l-Router neu starten. Wenn Sie also das erste Mal OpenVPN konfigurieren, tragen Sie alle Daten in die Konfigdatei ein und setzen entweder `OPENVPN_DEFAULT_CREATE_SECRET` (Seite 206) auf 'yes', wenn Sie gleich für alle OpenVPN Verbindungen neue Keyfiles erzeugen wollen oder nur für die entsprechende OpenVPN Verbindung `OPENVPN_x_CREATE_SECRET` auf 'yes'. Nach dem Start des fli4l-Routers werden dann die oder das Keyfile(s) automatisch erzeugt und in `/etc/openvpn` mit dem hier angegebenen Namen abgelegt. Das oder die Keyfile(s) kann dann per scp kopiert oder mit einer Diskette übertragen werden. Sie müssen nach dem Erstellen der Schlüsseldateien die Einstellung wieder auf 'no' setzen, das fli4l Bootmedium neu erzeugen und die neu erzeugte Konfiguration starten. Bleibt die Einstellung auf 'yes' werden bei jedem Start des fli4l-Routers neue Schlüsseldateien erzeugt aber kein OpenVPN Daemon gestartet. Es also kann kein Tunnel aufgebaut werden. Sie können `OPENVPN_x_CREATE_SECRET` auch auf 'webgui' setzen, wenn Sie die WebGUI verwenden möchten um Keyfile(s) zu generieren. Dazu müssen Sie in der WebGUI in die Detailansicht der Verbindung(en) gehen und den Punkt Keymanagement auswählen. Genauerer dazu im Abschnitt 4.15.6

Tip: Mit dem Kommando

```
openvpn --genkey --secret <dateiname>
```

können Sie ein Keyfile auf dem fli4l-Router auch von Hand erstellen.

Die Keyfiles müssen in das Verzeichnis `<config>/etc/openvpn` kopiert werden, wie in folgendem Bild zu sehen ist. Der Dateiname des Keyfiles ohne den Pfad muss anschließend in `OPENVPN_x_SECRET` hinterlegt werden. Dann werden die Keyfiles beim Erstellen des opt-Archives mit eingepackt.



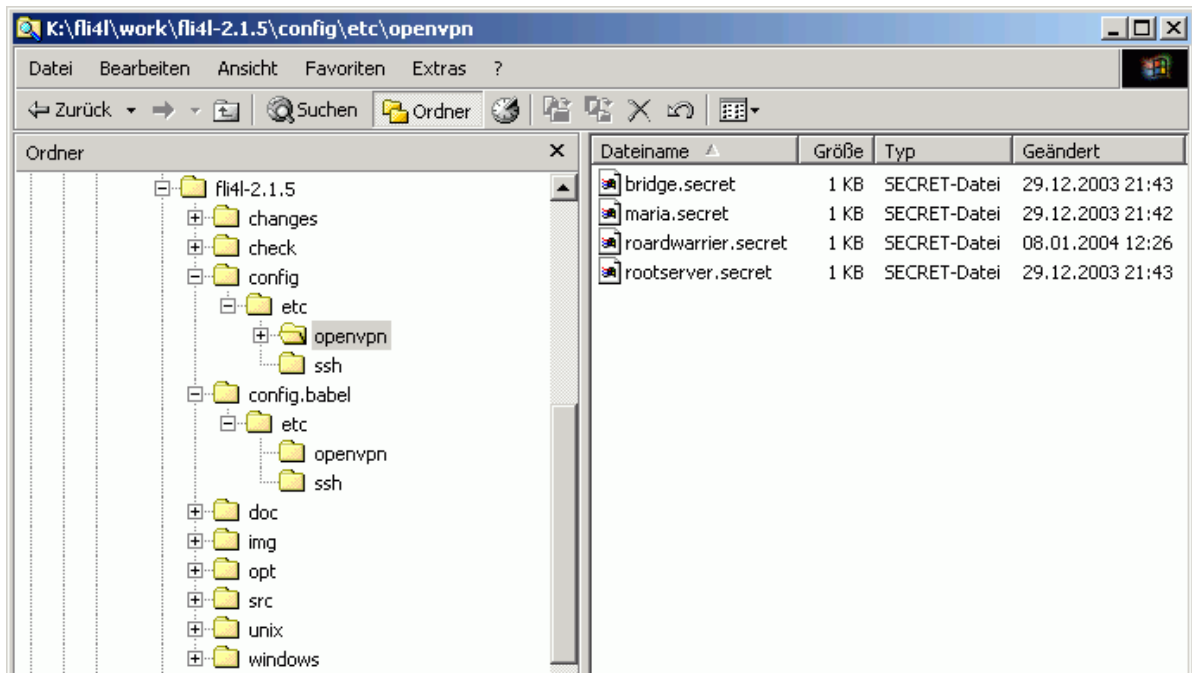


Abbildung 4.2.: fli4l config Directory mit OpenVPN \*.secret Dateien

**OPENVPN\_x\_TYPE** Default: OPENVPN\_x\_TYPE=""

Eine OpenVPN Verbindung kann entweder als Tunnel oder als Bridge benutzt werden. Über einen OpenVPN Tunnel kann ausschliesslich IP-Traffic geroutet werden. Über eine Bridge werden Ethernetframes übertragen, also nicht nur IP-Traffic, sondern z.B. auch IPX oder NetBEUI. Wenn OpenVPN als Transport für Ethernetframes benutzt werden soll, wird in jedem Fall noch das `advanced_networking` Paket benötigt. Bitte bedenken Sie, dass die Benutzung von Bridging über eine DSL Leitung sehr langsam werden kann!

**4.15.3. OpenVPN - Bridgekonfiguration**

Wenn Sie OpenVPN für eine Bridge benutzen wollen, sind folgende Einträge gültig. Bitte denken Sie daran, dass bei der Benutzung einer Bridge über das Internet der entstehende Broadcasttraffic unter Umständen schon eine relativ hohe Bandbreite benötigt.

Denken Sie daran, dass die folgenden Einstellungen nur gültig sind, wenn der `OPENVPN_x_TYPE` (Seite 201) für diese OpenVPN Verbindung auf 'bridge' eingestellt wurde! Ausserdem wird eine konfigurierte Bridge aus dem `advanced_networking` Paket benötigt, an die sich die VPN Verbindung hängen kann.

**OPENVPN\_x\_BRIDGE** Default: OPENVPN\_x\_BRIDGE=""

Hier wird der Name der Bridge angegeben, an die sich diese OpenVPN Verbindung hängen soll. Wenn also in `BRIDGE_DEV_x_NAME='cuj-br'` steht und sich diese OpenVPN Verbindung an diese Bridge hängen soll, muss hier ebenfalls 'cuj-br' angegeben werden.

**OPENVPN\_x\_BRIDGE\_COST** Default: OPENVPN\_x\_BRIDGE\_COST=""

Wenn Sie STP (siehe [http://de.wikipedia.org/wiki/Spanning\\_Tree](http://de.wikipedia.org/wiki/Spanning_Tree) oder die Dokumentation im `advanced_networking` Paket) benutzen, können Sie hier die Kosten der Verbindung angeben.

**OPENVPN\_x\_BRIDGE\_PRIORITY** Default: `OPENVPN_x_BRIDGE_PRIORITY=`"

Wenn Sie STP (siehe [http://de.wikipedia.org/wiki/Spanning\\_Tree](http://de.wikipedia.org/wiki/Spanning_Tree) oder die Dokumentation im `advanced_networking` Paket) benutzen, können Sie hier die Priorität der Verbindung angeben.

#### 4.15.4. OpenVPN - Tunnelkonfiguration

**OPENVPN\_x\_REMOTE\_VPN\_IP** Default: `OPENVPN_x_REMOTE_VPN_IP=`"

Diese Einstellung ist nur gültig, wenn der `OPENVPN_x_TYPE` (Seite 201) für diese OpenVPN Verbindung auf `'tunnel'` einstellt wurde!

Die VPN IP-Adresse der OpenVPN Gegenstelle. Die VPN IP-Adressen werden nur zum Routen benötigt und können fast frei gewählt werden. Es gelten dabei folgende Einschränkungen für die Auswahl der VPN IP-Adressen:

- Die IP-Adresse darf an keiner Stelle im lokalen Netz benutzt werden. Sie darf also nicht im Subnetz des `fli4l`-Routers liegen.
- Die IP-Adresse darf für kein lokales Netzwerkdevice benutzt werden.
- Die IP-Adresse darf nicht zu einem Netzwerk gehören, das mit `IP_ROUTE_x` geroutet wird.
- Die IP-Adresse darf nicht zu einem Netzwerk gehören, das mit `ISDN_CIRC_ROUTE_x` geroutet wird.
- Die IP-Adresse darf nicht zu einem Netzwerk gehören, das mit `CIPE_ROUTE_x` geroutet wird.
- Die IP-Adresse darf nicht zu einem Netzwerk gehören, das mit `OPENVPN_ROUTE_x` geroutet wird.
- Die IP-Adresse darf nicht zu einem Netzwerk gehören, das auf irgendeine andere Weise zum `fli4l` Netzwerk gehört oder vom `fli4l`-Router geroutet wird.

Wie Sie sehen darf die VPN IP-Adresse nirgends sonst benutzt werden. Bevor Sie mit der Konfiguration von OpenVPN beginnen, sollten Sie sich ein Netz suchen, was von keinem Netzwerk benutzt wird, in das Sie eine VPN Verbindung aufbauen wollen. Das Netzwerk sollte auch unbedingt zu einem der privaten Netze gehören (siehe <http://ftp.univie.ac.at/netinfo/rfc/rfc1597.txt>).

**OPENVPN\_x\_LOCAL\_VPN\_IP** Default: `OPENVPN_x_LOCAL_VPN_IP=`"

Diese Einstellung ist nur gültig, wenn der `OPENVPN_x_TYPE` (Seite 201) für diese OpenVPN Verbindung auf `'tunnel'` einstellt wurde.

Die IP-Adresse, die das lokale OpenVPN `tunX` Device bekommt. Für die Auswahl der IP-Adresse gelten die gleichen Einschränkungen wie bei `OPENVPN_x_REMOTE_VPN_IP` (Seite 202).

Es ist übrigens möglich, für alle lokalen OpenVPN Verbindungen die gleiche IP-Adresse bei `OPENVPN_x_LOCAL_VPN_IP` zu benutzen. So ist es problemlos möglich, dass ein Host in einem VPN immer die gleiche IP-Adresse benutzt. Das vereinfacht die Paketfilterregeln unter Umständen drastisch.

#### **OPENVPN\_x\_IPV6** Default: `OPENVPN_x_IPV6='no'`

Hiermit kann der native IPv6-Support von OpenVPN eingeschaltet werden. Da dieser Code noch recht neu ist, ist der Support als experimentell zu bezeichnen. Damit das Ganze einen Effekt hat, muss `OPT_IPV6` aktiviert und konfiguriert sein. Bei `OPENVPN_x_IPV6='no'` und/oder `OPT_IPV6='no'` werden die IPv6 relevanten Variablen ignoriert.

ACHTUNG!!! Zur Zeit gibt es hier keine Überprüfung ob sich die Angaben mit anderen Teilen der Konfiguration überschneiden! Dies gilt für `OPENVPN_x_LOCAL_VPN_IPV6`, `OPENVPN_x_REMOTE_VPN_IPV6` und `OPENVPN_x_ROUTE_x`.

#### **OPENVPN\_x\_REMOTE\_VPN\_IPV6** Default: `OPENVPN_x_REMOTE_VPN_IPV6=""`

Für die IPv6 gilt das Gleiche wie für die [OPENVPN\\_x\\_REMOTE\\_VPN\\_IP](#) (Seite 202).

```
OPENVPN_X_REMOTE_IPV6='FD00::1'
```

#### **OPENVPN\_x\_LOCAL\_VPN\_IPV6** Default: `OPENVPN_x_LOCAL_VPN_IPV6=""`

Für die IPv6 gilt das Gleiche wie für die [OPENVPN\\_x\\_LOCAL\\_VPN\\_IP](#) (Seite 202). Wird hier kein Subnetz gesetzt wird automatisch /64 als Subnetz genutzt.

```
OPENVPN_X_LOCAL_IPV6='FD00::2/112'
```

#### **OPENVPN\_x\_ROUTE\_N** Default: `OPENVPN_x_ROUTE_N=""`

Diese Einstellung ist nur gültig, wenn der [OPENVPN\\_x\\_TYPE](#) (Seite 201) für diese OpenVPN Verbindung auf `'tunnel'` eingestellt wurde.

Die angegebenen Routen werden automatisch von OpenVPN gesetzt, sobald OpenVPN gestartet wird. Es können bis zu 50 Netze über eine OpenVPN Verbindung geroutet werden. Sie müssen aber für jedes zu routende Netzwerk einen `OPENVPN_x_ROUTE_x` Eintrag erzeugen.

Bitte beachten Sie, dass Sie notwendige Paketfilterregeln in der `OPENVPN_PF_FORWARD_x`, `OPENVPN_PF_INPUT_x` bzw. `OPENVPN_PF6_FORWARD_x`, `OPENVPN_PF6_INPUT_x` bzw. selber setzen müssen. OpenVPN erlaubt nur ICMP über die VPN Verbindungen und verbietet allen anderen Datenverkehr. Details finden Sie unter [OPENVPN\\_x\\_PF\\_INPUT\\_N](#) (Seite 214) und [OPENVPN\\_x\\_PF\\_FORWARD\\_N](#) (Seite 215) bzw. unter [OPENVPN\\_x\\_PF6\\_INPUT\\_N](#) (Seite 215) und [OPENVPN\\_x\\_PF6\\_FORWARD\\_N](#) (Seite 215) bzw.

Für sehr spezielle Konfigurationen besteht die Möglichkeit, Skripte zu starten um z.B. Policy Based Routing zu ermöglichen. Die Skripte müssen dazu in dem Verzeichnis `config/etc/openvpn` abgelegt werden und folgendermaßen benannt werden:

#### 4. Pakete

<name>-<zeitpunkt>

Der “name” ist der Name der OpenVPN-Verbindung (OPENVPN\_x\_NAME). Für “zeitpunkt” stehen folgende Auswahlmöglichkeiten für die Ausführung der Skripte zur Verfügung:

up-pre Vor dem Herstellen der OpenVPN-Verbindung.

up-post Nach dem Herstellen der OpenVPN-Verbindung.

down-pre Vor dem Abbau der OpenVPN-Verbindung.

down-post Nach dem Abbau der OpenVPN-Verbindung.

route-up-pre Vor dem Setzen der OpenVPN-Routen.

route-up-post Nach dem Setzen der OpenVPN-Routen.

route-down-pre Vor dem Löschen der OpenVPN-Routen.

route-down-post Nach dem Löschen der OpenVPN-Routen.

Um ein Skript für die Verbindung OPENVPN\_x\_NAME='maria' nach dem Setzen der Routen zu starten muss ein Skript mit dem Namen `maria-route-up-post` in dem Verzeichnis `config/etc/openvpn` angelegt werden.

#### **OPENVPN\_x\_ROUTE\_x** Default: OPENVPN\_x\_ROUTE\_x="

Sie müssen hier die Netze angeben, die Sie über die OpenVPN Gegenstelle erreichen wollen. Sind hinter der OpenVPN Gegenstelle z.B. die Netzwerke 192.168.33.0/24 und 172.18.0.0/16 erreichbar und sollen diese über den OpenVPN Tunnel erreicht werden, müssen Sie diese beiden Netze jeweils einzeln unter OPENVPN\_x\_ROUTE\_x eintragen. Es können hier auch Hostrouten (/32) eingetragen werden.

Wenn die Defaultroute über einen OpenVPN Tunnel gesetzt werden soll, geben sie bitte 0.0.0.0/0 bzw. ::/0 für IPv6 und ein optionales Flag als Route an. Auch hier gilt, dass für IPv6 Routen OPT\_IPv6 aktiv sein muss, die lokale und remote IPv6-Adresse für den Tunnel müssen gesetzt sein und OPENVPN\_x\_IPV6 auf yes stehen. OpenVPN kennt verschiedene Möglichkeiten die Defaultroute einzurichten, die sie mit dem Flag auswählen können. Jede Methode, die Defaultroute einzurichten, hat ihre Vor- und Nachteile. Im Moment unterstützt OpenVPN folgende Flags:

**local** Das *local* Flag sollten sie wählen, wenn die OpenVPN Gegenstelle innerhalb eines direkt von ihrem fl4l-Router erreichbaren Subnetz liegt. Das ist z.B. oft bei einer Defaultroute mit OpenVPN über WLAN der Fall.

**def1** Mit diesem Flag werden zusätzliche zu einer Hostroute an die OpenVPN Gegenstelle zwei neue Routen, 0.0.0.0/1 und 128.0.0.0/1, eingetragen. Diese Routen übernehmen die Funktion einer Defaultroute und über diese Routen wird dann der komplette (verschlüsselte) Traffic an die OpenVPN Gegenstelle (die noch über die Hostroute erreichbar ist) geroutet.

Lassen Sie das optionale Flag weg wählt OpenVPN die Methode aus, wie die Defaultroute umgesetzt wird. Die Auswahl der Methode erfolgt dabei über die OpenVPN Version, im Moment wird als Standardeinstellung *local* benutzt.

OPENVPN\_1\_ROUTE\_N='3'

```
OPENVPN_1_ROUTE_1='192.168.33.0/24'  
OPENVPN_1_ROUTE_2='172.18.0.0/16'  
OPENVPN_1_ROUTE_3='2001:db8:/32'
```

### OpenVPN - Delegation von DNS und Reverse-DNS

**OPENVPN\_x\_DOMAIN** Default: OPENVPN\_x\_DOMAIN=""

Über diesen Parameter gibt man die Remote Domain an. Diese Variable kann mehrere Domains enthalten die durch Leerzeichen getrennt angegeben werden müssen. Wenn nur dieser Parameter gesetzt ist (ohne Angabe eines zusätzlichen DNS-Servers) wird davon ausgegangen, dass der DNS Server auf der IP des gegenüberliegenden Tunnelendes lauscht (siehe [OPENVPN\\_x\\_REMOTE\\_VPN\\_IP](#) (Seite 202)). Dazu müssen auf dem Remote Router natürlich eingehende DNS-Anfragen erlaubt werden. (z.B. via OPENVPN\_x\_INPUT\_y='tmp1:dns ACCEPT')

**OPENVPN\_x\_ROUTE\_x\_DOMAIN** Default: OPENVPN\_x\_ROUTE\_x\_DOMAIN=""

Den verschiedenen Subnetzen können auch verschiedene Domains zugeordnet sein. Hier kann man pro OPENVPN\_x\_ROUTE\_y eine entsprechende Domain konfigurieren. Sollte ein dazugehöriges OPENVPN\_x\_ROUTE\_y\_DNSIP existieren, so wird dieser Server benutzt, andernfalls der unter OPENVPN\_x\_DNSIP angegebene. Die Wirkung ist dann die selbe wie mit OPENVPN\_x\_DOMAIN, allerdings eignet sich diese Methode auch zur Dokumentation.

**OPENVPN\_x\_DNSIP** Default: OPENVPN\_x\_DNSIP=""

Ist der Tunnelendpunkt nicht der zuständige DNS-Server, so kann hier die IP des zuständigen DNS-Servers angegeben werden. Ist nichts angegeben, wird die unter [OPENVPN\\_x\\_REMOTE\\_VPN\\_IP](#) (Seite 202) angegebene IP benutzt.

**OPENVPN\_x\_ROUTE\_x\_DNSIP** Default: OPENVPN\_x\_ROUTE\_x\_DNSIP=""

Verschiedene geroutete Subnetze können auch durch verschiedene DNS-Server abgedeckt sein - hier kann man pro [OPENVPN\\_x\\_ROUTE\\_x](#) (Seite 204) einen eigenen zuständigen Server definieren.

### 4.15.5. Experteneinstellungen

Die in diesem Kapitel beschriebenen Einstellungen sind fast alle optional und sollten nur verändert werden, wenn die OpenVPN Verbindung mit den Standardeinstellungen funktioniert und Optimierungen (beispielsweise eine andere Schlüssellänge) vorgenommen werden sollen.

Mit Ausnahme von OPENVPN\_DEFAULT\_CIPHER und OPENVPN\_DEFAULT\_DIGEST sind alle nachfolgend beschriebenen OPENVPN\_DEFAULT\_ Einstellungen optional, d.h. diese Optionen brauchen nicht in die openvpn.txt Konfigurationsdatei geschrieben werden. Fehlt der entsprechende Eintrag in der openvpn.txt Datei, wird vom OpenVPN Startskript der hier angegebene Defaultwert benutzt. Wenn Sie nicht vorhaben die Standardwerte der Vorgaben zu ändern, schreiben Sie diese auch nicht in die openvpn.txt Konfigurationsdatei!

#### allgemeine Einstellungen

**OPENVPN\_DEFAULT\_CIPHER** Hier wird eine der verfügbaren Verschlüsselungsmethoden eingetragen. Zur Zeit werden die Verschlüsselungsmethoden in [Tab. 4.8](#) unterstützt.

Tabelle 4.8.: In OpenVPN verfügbare Verschlüsselungsmethoden

Kürzel	nominale Schlüssellänge	effektive Schlüssellänge	Bewertung
none	0 Bit	0 Bit	unsicher
DES-CBC	56 Bit	56 Bit	unsicher
DES-EDE-CBC	112 Bit	80 Bit	unsicher
DES-EDE3-CBC	168 Bit	112 Bit	unsicher
DESX-CBC	184 Bit	119 Bit	unsicher
RC2-40-CBC	40 Bit	40 Bit	unsicher
RC2-64-CBC	64 Bit	64 Bit	unsicher
RC2-CBC	128 Bit	128 Bit	unsicher
BF-CBC	128 Bit	128 Bit	sicher
CAST5-CBC	128 Bit	128 Bit	sicher
AES-128-CBC	128 Bit	128 Bit	sicher
AES-192-CBC	192 Bit	192 Bit	sicher
AES-256-CBC	256 Bit	256 Bit	sicher
CAMELLIA-128-CBC	128 Bit	128 Bit	sicher
CAMELLIA-192-CBC	192 Bit	192 Bit	sicher
CAMELLIA-256-CBC	256 Bit	256 Bit	sicher
SEED-CBC	128 Bit	128 Bit	sicher

**Wichtig:** Diese Variable hat keine Vorbelegung! Sie müssen somit einen Algorithmus auswählen. Falls Sie unsicher sind, wählen Sie

- “AES-128-CBC”, wenn Sie dafür Hardware-Unterstützung nutzen können (siehe Paket “hwsupp”), oder
- “AES-256-CBC”, wenn Sie eine schnelle CPU haben (1 GHz oder schneller), oder
- “BF-CBC” in allen anderen Fällen.

In alten Versionen von `fl4l` war diese Variable in der Standardeinstellung mit “BF-CBC” belegt.

**OPENVPN\_DEFAULT\_COMPRESS** Default: `OPENVPN_DEFAULT_COMPRESS='yes'`

OpenVPN benutzt eine adaptive LZO Datenkomprimierung, um die Bandbreite einer Verbindung zu erhöhen. Adaptiv bedeutet, dass OpenVPN selbstständig erkennt, wenn z.B. bereits gepackte ZIP Dateien über eine OpenVPN Verbindung geschickt werden. In einem solchen Fall wird die Datenkomprimierung solange abgeschaltet, bis wieder Daten übertragen werden, die auch von einer Datenkomprimierung profitieren. Es gibt fast nie einen Grund die Datenkomprimierung zu deaktivieren, da dadurch die Bandbreite quasi kostenlos erhöht wird. Einziger Nachteil der Datenkomprimierung ist eine geringe Erhöhung der Latenzzeit von wenigen Millisekunden. Für Online-Games via VPN, bei denen die Reaktionszeit (“guter” ping) entscheidend ist, wäre es also unter Umständen sinnvoll die Datenkomprimierung abzuschalten.

**OPENVPN\_DEFAULT\_CREATE\_SECRET** Default: `OPENVPN_DEFAULT_CREATE_SECRET='no'`

Mit dieser Einstellung erstellt OpenVPN automatisch Keyfiles beim Start des `fl4l`-Routers. Die entsprechende OpenVPN Verbindung wird allerdings nicht gestartet. Für

Details lesen Sie bitte den Punkt [OPENVPN\\_x\\_SECRET](#) (Seite 200) nach.

**OPENVPN\_DEFAULT\_DIGEST** Hier wird eine der verfügbaren Prüfsummenmethoden eingetragen. Zur Zeit werden die Prüfsummenmethoden in Tab. 4.9 unterstützt.

Tabelle 4.9.: In OpenVPN verfügbare Prüfsummenmethoden

Kürzel	Prüfsummenlänge	Bewertung
none	0 Bit	unsicher
MD4	128 Bit	unsicher
RSA-MD4	128 Bit	unsicher
MD5	128 Bit	unsicher
RSA-MD5	128 Bit	unsicher
MDC2	128 Bit	sicher
RSA-MDC2	128 Bit	sicher
SHA	160 Bit	unsicher
RSA-SHA	160 Bit	unsicher
SHA1	160 Bit	unsicher
RSA-SHA1	160 Bit	unsicher
DSA-SHA	160 Bit	unsicher
DSA-SHA1-old	160 Bit	unsicher
DSA-SHA1	160 Bit	unsicher
RSA-SHA1-2	160 Bit	unsicher
DSA	160 Bit	unsicher
RIPEMD160	160 Bit	sicher
RSA-RIPEMD160	160 Bit	sicher
ecdsa-with-SHA1	160 Bit	sicher
SHA224	224 Bit	sicher
RSA-SHA224	224 Bit	sicher
SHA256	256 Bit	sicher
RSA-SHA256	256 Bit	sicher
SHA384	384 Bit	sicher
RSA-SHA384	384 Bit	sicher
SHA512	512 Bit	sicher
RSA-SHA512	512 Bit	sicher
whirlpool	512 Bit	sicher

**Wichtig:** Diese Variable hat keine Vorbelegung! Sie müssen somit einen Algorithmus auswählen. Falls Sie unsicher sind, wählen Sie

- “whirlpool”, wenn Sie eine schnelle CPU haben (1 GHz oder schneller), oder
- “SHA256” sonst.

In alten Versionen von fli4l war diese Variable in der Standardeinstellung mit “SHA1” belegt.

**OPENVPN\_DEFAULT\_FLOAT** Default: OPENVPN\_DEFAULT\_FLOAT='yes'

Bei OpenVPN Verbindungen mit Gegenstellen, die eine DynDNS Adresse benutzen, ist es jederzeit möglich, dass sich die IP-Adresse der OpenVPN Gegenstelle ändert. Damit OpenVPN auch die geänderte IP-Adresse akzeptiert, muss `OPENVPN_DEFAULT_FLOAT` auf `'yes'` eingestellt werden. Mit der Einstellung `'no'` wird die Änderung der IP-Adresse nicht erlaubt. Das ist in der Regel nur bei WLAN Verbindungen oder OpenVPN Verbindungen mit Gegenstellen, die eine statische IP-Adresse (wie z.B. die rootserver diverser Anbieter) haben, sinnvoll. Sie können diese Einstellung auch wie alle anderen `OPENVPN_DEFAULT_` Einstellungen für eine bestimmte OpenVPN Verbindung überschreiben.

**OPENVPN\_DEFAULT\_KEYSIZE** Default: `OPENVPN_DEFAULT_KEYSIZE=""`

Die Schlüssellänge (=KEYSIZE) hängt von der verwendeten Verschlüsselungsmethode ab. Ändern Sie diese Einstellung nur, wenn Sie mit einer OpenVPN Gegenstelle zusammenarbeiten müssen, die nicht den Standardwert benutzt oder deren Einstellung Sie nicht beeinflussen können. Können Sie die Schlüssellänge selbst bestimmen, sollte dieser Wert immer leer bleiben. OpenVPN wendet dann eine optimale Schlüssellänge für die jeweilige Verschlüsselungsmethode an.

**OPENVPN\_DEFAULT\_OPEN\_OVPNPORT** Default: `OPENVPN_DEFAULT_OPEN_OVPNPORT='yes'`

Damit eine OpenVPN Gegenstelle mit Ihnen Kontakt aufnehmen kann, müssen Sie den Paketfilter Ihres fli4l-Routers entsprechend anpassen. In der Regel müssen Sie also auf allen TCP oder UDP Ports, je nach `OPENVPN_x_PROTOCOL` Einstellung, auf denen ein OpenVPN horcht, die `PF_INPUT_x` (Seite 49) in der base.txt anpassen. Mit der Einstellung `'yes'` werden diese Paketfilterregeln automatisch generiert. Bei einzelnen Verbindungen kann es aber durchaus Sinn machen, diese Einstellung auf `'no'` zu setzen und selber entsprechende Paketfilterregeln zu definieren.

**OPENVPN\_DEFAULT\_ALLOW\_ICMPING** Default: `OPENVPN_DEFAULT_ALLOW_ICMPING='yes'`

Mit `'yes'` wird der Paketfilter für die entsprechende Verbindung so konfiguriert, dass ping Datenpakete den Filter passieren dürfen. Wenn es keinen sehr wichtigen Grund gibt, sollte der ICMP Ping immer zugelassen werden. Diese Einstellung hat *nichts* mit der Pingoption von OpenVPN zu tun!

**OPENVPN\_DEFAULT\_PF\_INPUT\_LOG** Default: `OPENVPN_DEFAULT_PF_INPUT_LOG='BASE'`

Mit `'yes'` oder `'no'` wird eingestellt, ob der Paketfilter eingehende Datenpakete in der INPUT Liste, die für die entsprechende VPN Verbindung gedacht waren mitschreiben soll, wenn das Datenpaket abgelehnt wird. Mit der Einstellung `'BASE'` wird die Einstellung von `'PF_INPUT_LOG='` aus der base.txt übernommen.

**OPENVPN\_DEFAULT\_PF\_INPUT\_POLICY** Default: `OPENVPN_DEFAULT_PF_INPUT_POLICY='REJECT'`

Diese Einstellung entspricht `'PF_INPUT_POLICY='` (Seite 60) aus der base.txt. Zusätzlich zu den dort möglichen Einstellungen, kann mit `'BASE'` die Einstellung von `'PF_INPUT_POLICY='` aus der base.txt übernommen werden.

**OPENVPN\_DEFAULT\_PF\_FORWARD\_LOG** Default: `OPENVPN_DEFAULT_PF_FORWARD_LOG='BASE'`



Mit 'yes' oder 'no' wird eingestellt, ob der Paketfilter eingehende Datenpakete in der FORWARD Liste, die für die entsprechende VPN Verbindung gedacht waren mitschreiben soll, wenn das Datenpaket abgelehnt wird. Mit der Einstellung 'BASE' wird die Einstellung von 'PF\_FORWARD\_LOG=' aus der base.txt übernommen.

**OPENVPN\_DEFAULT\_PF\_FORWARD\_POLICY** Default: OPENVPN\_DEFAULT\_PF\_FORWARD\_POLICY='REJECT'

Diese Einstellung entspricht 'PF\_FORWARD\_POLICY=' (Seite 62) aus der base.txt. Zusätzlich zu den dort möglichen Einstellungen kann mit 'BASE' die Einstellung von 'PF\_FORWARD\_POLICY=' aus der base.txt übernommen werden.

**OPENVPN\_DEFAULT\_PING** Default: OPENVPN\_DEFAULT\_PING='60'

Um einen einmal aufgebauten Tunnel offen zu halten und zu erkennen, ob die OpenVPN Gegenstelle noch erreichbar ist, wird in dem angegebenen Intervall in Sekunden ein kryptografisch gesicherter ping über die Leitung geschickt. Mit der Einstellung 'off' schickt OpenVPN kein ping über die Leitung. Mit der Einstellung 'off' werden nur dann Daten über den VPN Tunnel geschickt wenn auch tatsächlich Nutzdaten über die VPN Tunnel übertragen werden.

**OPENVPN\_DEFAULT\_RENEG\_SEC** Default: OPENVPN\_DEFAULT\_RENEG\_SEC='3600'

Hiermit kann die Variable RENEG-SEC aus OpenVPN angepasst werden, so dass gerade bei langsamen DSL-Verbindungen (Oder ISDN) es nicht zu einem Timeout und Abbruch der Verbindung kommt.

**OPENVPN\_DEFAULT\_PING\_RESTART** Default: OPENVPN\_DEFAULT\_PING\_RESTART='180'

Wird in dem angegebenen Intervall in Sekunden kein OpenVPN ping erfolgreich über die VPN Verbindung geschickt oder werden keine anderen Daten übertragen, wird die entsprechende OpenVPN Verbindung neu gestartet. Der Wert von OPENVPN\_DEFAULT\_PING\_RESTART muss immer größer sein als der Wert von OPENVPN\_DEFAULT\_PING. Die Einstellung 'off' unterbindet den automatischen Neustart einer OpenVPN Verbindung.

**OPENVPN\_DEFAULT\_RESOLV\_RETRY** Default: OPENVPN\_DEFAULT\_RESOLV\_RETRY='infinite'

Sind in OPENVPN\_x\_REMOTE\_HOST oder OPENVPN\_x\_LOCAL\_HOST DNS Namen statt IP-Adressen hinterlegt, dann müssen die Namen beim Start einer OpenVPN Verbindung erst zu IP-Adressen aufgelöst werden. Sollte dies fehlschlagen, versucht OpenVPN für die angegebene Zeit in Sekunden die DNS Adresse erneut aufzulösen. Gelingt dies schlußendlich nicht in der vorgegebenen Zeit, kommt keine OpenVPN Verbindung zustande. Mit der Angabe 'infinite' (= unendlich) wird unendlich lange versucht, die DNS Auflösung vorzunehmen. Diese Einstellung sollte bis auf besondere Fälle nicht verändert werden!

**OPENVPN\_DEFAULT\_RESTART** Default: OPENVPN\_DEFAULT\_RESTART='ip-up'

Nach einer Trennung der Verbindung ist es sinnvoll, dass der entsprechende OpenVPN Tunnel sofort neu gestartet wird, damit die Unterbrechung des Tunnels möglichst kurz ist. Für alle OpenVPN Verbindungen, die über eine Wählverbindung wie DSL oder ISDN laufen, sollte hier 'ip-up' eingetragen werden. OpenVPN Verbindungen über eine WLAN Strecke dagegen sollten hier 'never' eintragen. In diesem Fall wird die Verbindung nicht nach einer Neueinwahl wieder gestartet, da ja die WLAN Verbindung unabhängig von

einer Einwahl ist. Wenn ein OpenVPN Tunnel über eine ISDN Wählverbindung mit `ISDN_CIRC_x_TYPE='raw'` aufgebaut werden soll, muss hier `'raw-up'` eingetragen werden.

#### **OPENVPN\_DEFAULT\_PROTOCOL** Default: `OPENVPN_DEFAULT_PROTOCOL='udp4'`

Mit dieser Variablen wird festgelegt, welche Protokollvariante als Default benutzt werden soll. Normalerweise ist UDP eine sehr gute Wahl, allerdings gibt es manchmal nur die Möglichkeit mit TCP zu arbeiten. Der dadurch entstehende Overhead ist allerdings beachtlich. Mögliche Einstellungen sind `'udp4'`, `'udp6'`, `'tcp4-server'`, `'tcp6-server'`, `'tcp4-client'` oder `'tcp6-client'`. Die `'tcp[46]-server'`- oder `'tcp[46]-client'`-Einstellungen sind in der Regel nur dann sinnvoll, wenn ein VPN Tunnel durch div. andere Paketfilter oder andere Tunnel aufgebaut werden soll. Wenn Sie keine Spezialfälle behandeln müssen, sollten Sie *immer* den Standardwert `'udp4'` bzw. `'udp6'` benutzen.

#### **OPENVPN\_DEFAULT\_START** Default: `OPENVPN_DEFAULT_START='always'`

Eine OpenVPN Verbindung kann entweder immer (`'always'`) oder später von Hand (`'on-demand'`) gestartet werden. Sie können also bestimmte OpenVPN Verbindungen erst bei Bedarf über die OpenVPN WebGUI (siehe [4.15.6](#)) starten. Alternativ ist der Start aber auch jederzeit über die fli4l Konsole möglich. Melden Sie sich dazu auf der fli4l Konsole an und führen Sie folgende Befehle direkt auf der Konsole aus:

```
cd /etc/openvpn
openvpn --config name.conf --daemon openvpn-name
```

Damit wird ein OpenVPN Tunnel gestartet, der ab sofort im Hintergrund läuft. Anstelle `name.conf` nehmen Sie natürlich den Namen Ihrer Konfigurationsdatei in dem `/etc/openvpn` Verzeichnis.

#### **OPENVPN\_DEFAULT\_VERBOSE** Default: `OPENVPN_DEFAULT_VERBOSE='2'`

Diese Variable gibt an, wie geschwätzig OpenVPN sein soll. Wenn eine VPN Verbindung einwandfrei läuft, ist es möglich diesen Wert auf `'0'` zu setzen, um alle Meldungen zu unterbinden. Für die ersten Tests ist ein Wert von `'3'` sinnvoll. Noch größere Werte erhöhen die Debugmeldungen und helfen unter Umständen Fehler zu finden. Der Maximalwert beträgt `'11'`.

#### **OPENVPN\_DEFAULT\_MANAGEMENT\_LOG\_CACHE** Default:

`OPENVPN_DEFAULT_MANAGEMENT_LOG_CACHE='100'`

Diese Variable gibt an, wie viele Log Zeilen gespeichert werden sollen. Dieses Log kann dann über die [WebGUI](#) (Seite [216](#)) abgefragt werden.

#### **OPENVPN\_DEFAULT\_MUTE\_REPLAY\_WARNINGS** Default:

`OPENVPN_DEFAULT_MUTE_REPLAY_WARNINGS='no'`

Mit dieser Variablen wird eingestellt, ob beim Empfang doppelter Pakete eine Warnung im Log ausgegeben werden soll, da dies Hinweise auf ein Sicherheitsproblem im Netzwerk sein können. Insbesondere bei schwachen WLAN-Verbindungen, kann es aber häufig passieren, dass Pakete doppelt gesendet werden. Dann ist es sinnvoll die Warnungen auszustellen, damit diese nicht das Log füllen. Die Einstellung dieser Variablen hat *keinen* Einfluss auf die Sicherheit der OpenVPN Verbindung.

### **OPENVPN\_DEFAULT\_MSSFIX** Default: `OPENVPN_DEFAULT_MSSFIX=""`

Mit der MSSFIX Einstellung wird die Größe der TCP Datenpakete über die VPN Verbindung vorgegeben. Mit `OPENVPN_DEFAULT_MSSFIX='0'` wird diese Option ausgeschaltet. Wird eine Fragmentgröße angegeben und der MSSFIX Eintrag leer gelassen, wird automatisch die Fragmentgröße benutzt. Diese Einstellung funktioniert nur, wenn `OPENVPN_x_PROTOCOL='udp4'` oder `OPENVPN_x_PROTOCOL='udp6'` gesetzt wird.

### **OPENVPN\_DEFAULT\_FRAGMENT** Default: `OPENVPN_DEFAULT_FRAGMENT='1300'`

Aktiviert die interne Fragmentierung von OpenVPN mit einer Paketgröße von x Bytes. Diese Einstellung funktioniert nur, wenn `OPENVPN_x_PROTOCOL='udp4'` oder `OPENVPN_x_PROTOCOL='udp6'` gesetzt wird.

Mit `OPENVPN_DEFAULT_FRAGMENT='0'` wird die Fragmentierung komplett deaktiviert.

### **OPENVPN\_DEFAULT\_TUN\_MTU** Default: `OPENVPN_DEFAULT_TUN_MTU='1500'`

Stellt die MTU des virtuellen OpenVPN Adapters auf x Bytes ein. Diese Option sollte nur geändert werden, wenn man weiss was man macht. Es ist meistens sinnvoller, erst mit den Fragment oder MSSFIX Optionen zu arbeiten.

### **OPENVPN\_DEFAULT\_TUN\_MTU\_EXTRA** Default: `OPENVPN_DEFAULT_TUN_MTU_EXTRA=""`

Wenn bei `OPENVPN_x_PROTOCOL='bridge'` eingestellt wird, werden 32 Bytes als extra Speicher für die Verwaltung der Puffers für das tap Gerät reserviert. Bei `OPENVPN_x_PROTOCOL='tunnel'` wird kein extra Speicher reserviert. Diese Einstellung wirkt sich nur auf den Speicherbedarf im Router aus und hat keinen Einfluss auf die Datenmenge die über den Tunnel verschickt wird.

### **OPENVPN\_DEFAULT\_LINK\_MTU** Default: `OPENVPN_DEFAULT_LINK_MTU=""`

Stellt die MTU der OpenVPN Verbindung auf x Bytes ein. Diese Option sollte nur benutzt werden, wenn man weiss was man macht. Es ist meistens sinnvoller erst mit den Fragment oder MSSFIX Optionen zu arbeiten.

### **OPENVPN\_DEFAULT\_SHAPER** Default: `OPENVPN_DEFAULT_SHAPER=""`

Begrenzt die *ausgehende* Bandbreite des Tunnel auf die angegebene Anzahl von Bytes pro Sekunde. Möglich sind Werte von 100 Bytes bis zu 100000000 Bytes. Bei Werten bis 1000 Bytes pro Sekunde sollten Sie die MTU der Verbindung reduzieren, sonst steigen die ping Zeiten stark an. Wenn Sie einen Tunnel auf eine Bandbreite in beide Richtungen begrenzen wollen, müssen Sie dies auf beiden Seiten getrennt einstellen.

In der aktuellen OpenVPN Version funktioniert das Shaping nicht korrekt, d.h. die Übertragungsrate durch einen mittels Shapping konfigurierten Tunnel ist unter Umständen extrem schwankend bzw. der Durchsatz bricht total ein. Das Problem kann je nach eingesetzter Hardware auftreten zu komplett unterschiedlichen Verhalten führen. Im Moment sollte die Shappingfunktion mit Vorsicht behandelt werden und im Zweifel bei jeder Änderung ausgiebig getestet werden.

### **OPENVPN\_EXPERT** Default: `OPENVPN_EXPERT='no'`

Der Expert-Mode erlaubt Ihnen, native Openvpn Konfigurationsdateien zu nutzen. Diese müssen im Konfigurationsordner unter `etc/openvpn` sowie `etc/openvpn/scripts` abgelegt werden. Alle dort liegenden Dateien werden auf den Router übertragen.

Der Expert-Mode ignoriert die restlichen Konfigurationseinstellungen. Deshalb muss `OPENVPN_N=0` eingestellt werden.

Der Expert-Mode richtet keinerlei Firewall-Regeln ein. Diese müssen Sie manuell in die `base.txt` eintragen.

### verbindungsspezifische Einstellungen

Die folgenden OpenVPN Optionen gelten nur für die jeweilige OpenVPN Verbindung. Auch hier gibt es nur wenige Angaben, die zwingend sind. Die meisten Optionen können einfach weggelassen werden. Für alle Defaultwerte gilt, dass diese von der jeweils gleichlautenden `OPENVPN_DEFAULT_x` Einstellung übernommen werden. Wenn Sie also den entsprechenden `OPENVPN_DEFAULT_` Wert ändern, gilt dieser Defaultwert für alle OpenVPN Verbindungen, die den allgemeinen Defaultwert nicht überschreiben.

#### **OPENVPN\_x\_NAME** Default: `OPENVPN_x_NAME=""`

Legt einen bis zu 16 Zeichen langen Namen für die jeweilige OpenVPN Verbindung fest. Unter diesem Namen wird die Konfigurationsdatei im Verzeichnis `/etc/openvpn` (mit dem Anhang `.conf`) angelegt. Außerdem erscheint der Name im syslog. Wenn Sie beispielsweise den Namen `'peter'` eintragen, taucht später im syslog der Eintrag `'openvpn-peter'` auf. Damit können Sie die verschiedenen OpenVPN Verbindungen gut auseinanderhalten. Der Name darf Buchstaben, Zahlen und das `'-'` Zeichen enthalten.

#### **OPENVPN\_x\_ACTIV** Default: `OPENVPN_x_ACTIV='yes'`

Wenn man eine OpenVPN Verbindung deaktivieren, aber die Konfiguration nicht löschen will, kann diese OpenVPN Verbindung mit der Einstellung `'no'` deaktiviert werden. Die Konfigurationsdaten werden dann zwar in der `rc.cfg` aufgenommen, aber es wird keine entsprechende OpenVPN Verbindung erzeugt.

#### **OPENVPN\_x\_CHECK\_CONFIG** Default: `OPENVPN_x_CHECK_CONFIG='yes'`

Die erweiterten Prüfungen von OpenVPN sind in seltenen Fällen zu streng. Wenn beispielsweise eine ISDN Backupverbindung die gleichen Routingeinträge benutzt wie eine Verbindung, die über das Internet läuft, wird die erweiterte Prüfung diese Verbindungen mit einer Fehlermeldung bedenken. In diesem Fall sollte bei der Backupverbindung die erweiterte Prüfung deaktiviert werden. Dazu setzen Sie `OPENVPN_x_CHECK_CONFIG='no'`, um die Prüfungen für diese Verbindung auszuschalten.

#### **OPENVPN\_x\_CIPHER** Default siehe: `OPENVPN_DEFAULT_CIPHER`

Siehe [OPENVPN\\_DEFAULT\\_CIPHER](#) (Seite 205). Im Gegensatz zu der Default Einstellung wirkt diese Einstellung nur auf diese OpenVPN Verbindung.

#### **OPENVPN\_x\_COMPRESS** Default siehe: `OPENVPN_DEFAULT_COMPRESS`

Siehe [OPENVPN\\_DEFAULT\\_COMPRESS](#) (Seite 206). Im Gegensatz zu der Default Einstellung wirkt diese Einstellung nur auf diese OpenVPN Verbindung.

#### **OPENVPN\_x\_CREATE\_SECRET** Default siehe: `OPENVPN_DEFAULT_CREATE_SECRET='no'`

Siehe [OPENVPN\\_x\\_SECRET](#) (Seite 200). Im Gegensatz zu der Default Einstellung wirkt diese Einstellung nur auf diese OpenVPN Verbindung.

**OPENVPN\_x\_DIGEST** Default siehe: OPENVPN\_DEFAULT\_DIGEST

Siehe [OPENVPN\\_DEFAULT\\_DIGEST](#) (Seite 207). Im Gegensatz zu der Default Einstellung wirkt diese Einstellung nur auf diese OpenVPN Verbindung.

**OPENVPN\_x\_FLOAT** Default siehe: OPENVPN\_DEFAULT\_FLOAT

Siehe [OPENVPN\\_DEFAULT\\_FLOAT](#) (Seite 207). Im Gegensatz zu der Default Einstellung wirkt diese Einstellung nur auf diese OpenVPN Verbindung.

**OPENVPN\_x\_KEYSIZE** Default siehe: OPENVPN\_DEFAULT\_KEYSIZE

Siehe [OPENVPN\\_DEFAULT\\_KEYSIZE](#) (Seite 208). Im Gegensatz zu der Default Einstellung wirkt diese Einstellung nur auf diese OpenVPN Verbindung.

**OPENVPN\_x\_ISDN\_CIRC\_NAME** Default OPENVPN\_x\_ISDN\_CIRC\_NAME=""

Gibt an über welchen ISDN Circuit diese OpenVPN Verbindung aufgebaut wird. Hier wird der Name des entsprechenden ISDN Circuits eingetragen, der mit [ISDN\\_CIRC\\_x\\_NAME=""](#) (Seite 184) definiert wird. Der entsprechende ISDN Circuit muss dabei vom Typ 'raw' sein.

**OPENVPN\_x\_PING** Default siehe: OPENVPN\_DEFAULT\_PING

Siehe [OPENVPN\\_DEFAULT\\_PING](#) (Seite 209). Im Gegensatz zu der Default Einstellung wirkt diese Einstellung nur auf diese OpenVPN Verbindung.

**OPENVPN\_x\_PROTOCOL** Default: OPENVPN\_x\_PROTOCOL='udp4'

Gibt an mit welchem Protokoll der OpenVPN Tunnel aufgebaut werden soll. Mögliche Einstellungen sind 'udp4', 'udp6', 'tcp4-server', 'tcp6-server', 'tcp4-client' oder 'tcp6-client'. Die 'tcp[46]-server'- oder 'tcp[46]-client'-Einstellungen sind in der Regel nur dann sinnvoll, wenn ein VPN Tunnel durch diverse andere Paketfilter oder andere Tunnel aufgebaut werden soll. Wenn Sie keine Spezialfälle behandeln müssen, sollten Sie *immer* den Standardwert 'udp4' bzw. 'udp6' benutzen.

**OPENVPN\_x\_RESOLV\_RETRY** Default siehe: OPENVPN\_DEFAULT\_RESOLV\_RETRY

Siehe [OPENVPN\\_DEFAULT\\_RESOLV\\_RETRY](#) (Seite 209). Im Gegensatz zu der Default Einstellung wirkt diese Einstellung nur auf diese OpenVPN Verbindung.

**OPENVPN\_x\_PING\_RESTART** Default siehe: OPENVPN\_DEFAULT\_PING\_RESTART

Siehe [OPENVPN\\_DEFAULT\\_PING\\_RESTART](#) (Seite 209). Im Gegensatz zu der Default Einstellung wirkt diese Einstellung nur auf diese OpenVPN Verbindung.

**OPENVPN\_x\_START** Default siehe: OPENVPN\_DEFAULT\_START

Siehe [OPENVPN\\_DEFAULT\\_START](#) (Seite 210). Im Gegensatz zu der Default Einstellung wirkt diese Einstellung nur auf diese OpenVPN Verbindung.

**OPENVPN\_x\_VERBOSE** Default siehe: OPENVPN\_DEFAULT\_VERBOSE

Siehe [OPENVPN\\_DEFAULT\\_VERBOSE](#) (Seite 210). Im Gegensatz zu der Default Einstellung wirkt diese Einstellung nur auf diese OpenVPN Verbindung.

**OPENVPN\_x\_MANAGEMENT\_LOG\_CACHE** Default siehe:  
OPENVPN\_DEFAULT\_MANAGEMENT\_LOG\_CACHE

Siehe [OPENVPN\\_DEFAULT\\_MANAGEMENT\\_LOG\\_CACHE](#) (Seite 210). Im Gegensatz zu der Default Einstellung wirkt diese Einstellung nur auf diese OpenVPN Verbindung.

**OPENVPN\_x\_MUTE\_REPLAY\_WARNINGS** Default siehe:  
OPENVPN\_DEFAULT\_MUTE\_REPLAY\_WARNINGS

Siehe [OPENVPN\\_DEFAULT\\_MUTE\\_REPLAY\\_WARNINGS](#) (Seite 210). Im Gegensatz zu der Default Einstellung wirkt diese Einstellung nur auf diese OpenVPN Verbindung.

**OPENVPN\_x\_RESTART** Default siehe: OPENVPN\_DEFAULT\_RESTART

Siehe [OPENVPN\\_DEFAULT\\_RESTART](#) (Seite 209). Im Gegensatz zu der Default Einstellung wirkt diese Einstellung nur auf diese OpenVPN Verbindung.

**OPENVPN\_x\_ALLOW\_ICMPPING** Default siehe: OPENVPN\_DEFAULT\_ALLOW\_ICMPPING

Siehe [OPENVPN\\_DEFAULT\\_ALLOW\\_ICMPPING](#) (Seite 208). Im Gegensatz zu der Default Einstellung wirkt diese Einstellung nur auf diese OpenVPN Verbindung.

**OPENVPN\_x\_OPEN\_OVPNPORT** Default siehe: OPENVPN\_DEFAULT\_OPEN\_OVPNPORT

Siehe [OPENVPN\\_DEFAULT\\_OPEN\\_OVPNPORT](#) (Seite 208). Im Gegensatz zu der Default Einstellung wirkt diese Einstellung nur auf diese OpenVPN Verbindung.

**OPENVPN\_x\_PF\_INPUT\_LOG** Default siehe: OPENVPN\_DEFAULT\_PF\_INPUT\_LOG

Siehe [OPENVPN\\_DEFAULT\\_PF\\_INPUT\\_LOG](#) (Seite 208). Im Gegensatz zu der Default Einstellung wirkt diese Einstellung nur auf diese OpenVPN Verbindung.

**OPENVPN\_x\_PF\_INPUT\_POLICY** Default siehe: OPENVPN\_DEFAULT\_PF\_INPUT\_POLICY

Siehe [OPENVPN\\_DEFAULT\\_PF\\_INPUT\\_POLICY](#) (Seite 208). Im Gegensatz zu der Default Einstellung wirkt diese Einstellung nur auf diese OpenVPN Verbindung.

**OPENVPN\_x\_PF\_INPUT\_N** Default: OPENVPN\_x\_PF\_INPUT\_N='0'

Gibt die Anzahl der folgenden OPENVPN\_x\_PF\_INPUT\_x= Einträge an.

**OPENVPN\_x\_PF\_INPUT\_x** Default: OPENVPN\_x\_PF\_INPUT\_x=""

Wie im base Paket stehen hier die Anweisungen für den Paketfilter. Es wird genau die gleiche Syntax wie in base.txt benutzt. Auch tmpl: und Hostalias sind möglich. Zusätzlich gibt es noch die Möglichkeit, einige spezielle symbolische Namen zu benutzen. Es werden folgende symbolische Namen unterstützt:

**VPNDEV** Entspricht dem aktuellen tun Device der jeweiligen OpenVPN Verbindung.

**LOCAL-VPN-IP** Setzt die IP-Adresse von OPENVPN\_x\_LOCAL\_VPN\_IP ein.

**REMOTE-VPN-IP** Setzt die IP-Adresse von OPENVPN\_x\_REMOTE\_VPN\_IP ein.

**REMOTE-NET** Setzt die IP-Adresse von OPENVPN\_x\_REMOTE\_VPN\_IP ein und zusätzlich noch alle Netze die mit OPENVPN\_x\_ROUTE\_x angegeben wurden.

**OPENVPN\_x\_PF\_FORWARD\_LOG** Default siehe: `OPENVPN_DEFAULT_PF_FORWARD_LOG`

Siehe [OPENVPN\\_DEFAULT\\_PF\\_FORWARD\\_LOG](#) (Seite 208). Im Gegensatz zu der Default Einstellung wirkt diese Einstellung nur auf diese OpenVPN Verbindung.

**OPENVPN\_x\_PF\_FORWARD\_POLICY** Default siehe: `OPENVPN_DEFAULT_PF_FORWARD_POLICY`

Siehe [OPENVPN\\_DEFAULT\\_PF\\_FORWARD\\_POLICY](#) (Seite 208). Im Gegensatz zu der Default Einstellung wirkt diese Einstellung nur auf diese OpenVPN Verbindung.

**OPENVPN\_x\_PF\_FORWARD\_N** Default: `OPENVPN_x_PF_FORWARD_N='0'`

Gibt die Anzahl der folgenden `OPENVPN_x_PF_FORWARD_x` Einträge an.

**OPENVPN\_x\_PF\_FORWARD\_x** Default: `OPENVPN_x_PF_FORWARD_x=""`

Siehe [OPENVPN\\_x\\_PF\\_INPUT\\_x](#) (Seite 214).

**OPENVPN\_x\_PF\_PREROUTING\_N** Default: `OPENVPN_x_PF_PREROUTING_N='0'`

Gibt die Anzahl der folgenden `OPENVPN_x_PF_PREROUTING_x` Einträge an.

**OPENVPN\_x\_PF\_PREROUTING\_x** Default: `OPENVPN_x_PF_PREROUTING_x=""`

Siehe [OPENVPN\\_x\\_PF\\_INPUT\\_x](#) (Seite 214).

**OPENVPN\_x\_PF\_POSTROUTING\_N** Default: `OPENVPN_x_PF_POSTROUTING_N='0'`

Gibt die Anzahl der folgenden `OPENVPN_x_PF_POSTROUTING_x` Einträge an.

**OPENVPN\_x\_PF\_POSTROUTING\_x** Default: `OPENVPN_x_PF_POSTROUTING_x=""`

Ab fli4l Revision 3.5.0 (oder 3.5.0-rev18133 für tarball Benutzer) ergibt sich eine Änderung im Verhalten. War es früher möglich Einträge in der Form von

`OPENVPN_1_PF_POSTROUTING_1='MASQUERADE'`

anzugeben wird ab jetzt die Angabe einer Quell und Zieladresse erzwungen. Dies ist notwendig geworden, weil die POSTROUTING Regeln sonst nicht im vollem Umfang genutzt werden konnten. In den meisten Fällen reicht es einfach die Regeln und [IP\\_NET\\_x](#) (Seite 41) und REMOTE-NET zu ergänzen.

Siehe [OPENVPN\\_x\\_PF\\_INPUT\\_x](#) (Seite 214).

**OPENVPN\_x\_PF6\_INPUT\_N** Default: `OPENVPN_x_PF6_INPUT_N='0'`

Gibt die Anzahl der folgenden `OPENVPN_x_PF6_INPUT_x` Einträge an.

**OPENVPN\_x\_PF6\_INPUT\_x** Default: `OPENVPN_x_PF6_INPUT_x=""`

Wie im IPv6 Paket stehen hier die Anweisungen für den Paketfilter. Es wird genau die gleiche Syntax wie in `ipv6.txt` benutzt. Auch `tmpl:` und Hostalias sind möglich. Zusätzlich gibt es noch die Möglichkeit, einige spezielle symbolische Namen zu benutzen. Siehe dazu [OPENVPN\\_x\\_PF\\_INPUT\\_x](#) (Seite 214)

**OPENVPN\_x\_PF6\_FORWARD\_N** Default: `OPENVPN_x_PF6_FORWARD_N='0'`

Gibt die Anzahl der folgenden `OPENVPN_x_PF6_FORWARD_x` Einträge an.



**OPENVPN\_x\_PF6\_FORWARD\_x** Default: `OPENVPN_x_PF6_FORWARD_x=""`

Siehe [OPENVPN\\_x\\_PF6\\_INPUT\\_x](#) (Seite 215).

**OPENVPN\_x\_MSSFIX** Default siehe: `OPENVPN_DEFAULT_MSSFIX`

Siehe [OPENVPN\\_DEFAULT\\_MSSFIX](#) (Seite 211). Im Gegensatz zu der Default Einstellung wirkt diese Einstellung nur auf diese OpenVPN Verbindung.

**OPENVPN\_x\_CHECK\_REPLAY** Default: `OPENVPN_x_CHECK_REPLAY='yes'`

OpenVPN verhindert standardmäßig verschiedene Arten von Replayattacken. Replayattacken sind vereinfacht gesagt die böswillige Manipulation einer OpenVPN Verbindung durch Einfügen von alten Datenpaketen in eine vorhandene OpenVPN-Verbindung. In seltenen Fällen kann es notwendig sein diese Schutzfunktion zu deaktivieren um eine Verbindung mit bestimmten Gegenstellen zu ermöglichen. In diesen Fällen lässt sich die Schutzfunktion deaktivieren durch Setzen von

`OPENVPN_x_CHECK_REPLAY='no'`

**OPENVPN\_x\_FRAGMENT** Default siehe: `OPENVPN_DEFAULT_FRAGMENT`

Siehe [OPENVPN\\_DEFAULT\\_FRAGMENT](#) (Seite 211). Im Gegensatz zu der Default Einstellung wirkt diese Einstellung nur auf diese OpenVPN Verbindung.

**OPENVPN\_x\_TUN\_MTU** Default siehe: `OPENVPN_DEFAULT_TUN_MTU`

Siehe [OPENVPN\\_DEFAULT\\_TUN\\_MTU](#) (Seite 211). Im Gegensatz zu der Default Einstellung wirkt diese Einstellung nur auf diese OpenVPN Verbindung.

**OPENVPN\_x\_TUN\_MTU\_EXTRA** Default siehe: `OPENVPN_DEFAULT_TUN_MTU_EXTRA`

Siehe [OPENVPN\\_DEFAULT\\_TUN\\_MTU\\_EXTRA](#) (Seite 211). Im Gegensatz zu der Default Einstellung wirkt diese Einstellung nur auf diese OpenVPN Verbindung.

**OPENVPN\_x\_LINK\_MTU** Default siehe: `OPENVPN_DEFAULT_LINK_MTU`

Siehe [OPENVPN\\_DEFAULT\\_LINK\\_MTU](#) (Seite 211). Im Gegensatz zu der Default Einstellung wirkt diese Einstellung nur auf diese OpenVPN Verbindung.

**OPENVPN\_x\_SHAPER** Default siehe: `OPENVPN_DEFAULT_SHAPER=""`

Siehe [OPENVPN\\_DEFAULT\\_SHAPER](#) (Seite 211). Im Gegensatz zu der Default Einstellung wirkt diese Einstellung nur auf diese OpenVPN Verbindung.

#### 4.15.6. OpenVPN - WebGUI

Seit der Version 2.1.10 ist es möglich über eine WebGUI, die konfigurierten OpenVPN Verbindungen zu starten, stoppen und andere grundlegende Funktionen auszuführen. Dazu wird das `mini_httpd` Paket benötigt. Zudem muss die Variable `OPENVPN_WEBGUI` in der `openvpn.txt` auf 'yes' gesetzt werden. Dann wird der fli4l Weboberfläche der Menüpunkt OpenVPN hinzugefügt. Wählt man diesen Menüpunkt an, erscheint eine Übersicht über die konfigurierten OpenVPN Verbindungen, deren Status und die jeweils zur Verfügung stehenden Aktionen (siehe Abbildung 4.3).



OpenVPN-Verbindungen		
Status	Name	Aktion
 Verbunden	<a href="#">ktbs</a>	  
 Verbindung getrennt	<a href="#">kthan</a>	
 Verbindung angehalten	<a href="#">wlan-ellen</a>	  
 Verbindung getrennt	<a href="#">wlan-qast</a>	
 Verbindung wird aufgebaut ...	<a href="#">wlan-helmut</a>	  

Abbildung 4.3.: Verbindungsübersicht

**OpenVPN - WebGUI - Verbindungsübersicht**

**Status:** Der Status einer Verbindung wird mit Ampelmännchen symbolisiert. Ein rotes Männchen bedeutet, dass der OpenVPN-Prozess nicht läuft, ein gelbes, dass der Prozess zwar läuft aber (noch) keine Verbindung zur Gegenstelle aufgebaut werden konnte und ein grünes, dass die Verbindung mit der Gegenstelle „steht“. Genauere Informationen über den Status erhält man als Tooltip über dem Ampelmännchen. Das kann insbesondere bei „gelbem“ Status aufschlussreich sein.

**Name:** In dieser Spalte steht der Name der OpenVPN-Verbindung wie er in der Konfiguration angegeben wurde. Ein Klick auf den Namen führt in eine Übersicht, in der genauere Informationen zu dieser Verbindung angezeigt werden. Dazu später mehr.

**Aktion:** Hier sind die zur Verfügung stehenden Aktionen als Buttons symbolisiert. Was sie jeweils bedeuten, erfährt man über Tooltips. Folgende Buttons gibt es:

**OpenVPN - WebGUI - Detailansicht einer Verbindung**

**Statistik:** Hier werden ein paar interessante Statistiken angezeigt. Die Statistik kann nur angezeigt werden, wenn die Verbindung gestartet und nicht angehalten ist.

**Log:** Zeigt die letzten 20 Zeilen des Verbindungslogs. Wenn Sie mehr Zeilen sehen möchten,

Symbol	Erläuterung
	Der OpenVPN-Prozess wird gestartet und es wird versucht eine Verbindung aufzubauen.
	Der OpenVPN-Prozess wird beendet.
	Die Verbindung wird zurückgesetzt.
	Die Verbindung wird zurückgesetzt und auf 'hold' geschaltet. Dann gehen keine Daten mehr über die Verbindung.
	Die Verbindung wird wieder freigegeben. Daten können wieder über die Verbindung fließen.



Tabelle 4.10.: Aktionen der OpenVPN-Webgui



Abbildung 4.4.: Detailansicht einer Verbindung (Keymanagement)

können Sie auch deren Anzahl angeben und auf 'Anzeigen' klicken. Wenn Sie als Anzahl 'all' eingeben, wird das gesamte Log angezeigt. Dieser Reiter wird nur angezeigt, wenn die Verbindung gestartet ist.

**Debug-Log:** Zeigt die Ausgabe eines Startvorgangs. Die OpenVPN-Verbindung wird gestartet und die Ausgaben dabei angezeigt. Das ist dann nützlich, wenn die Verbindung über den Start Button nicht starten will und man dadurch kein normales Log zu sehen bekommt. Dieser Reiter wird nur angezeigt, wenn die Verbindung nicht gestartet ist.

**Paketfilter:** Zeigt die Paketfilterkonfiguration an, die für diese Verbindung gültig ist. Der Paketfilter ist nur konfiguriert, wenn die Verbindung gestartet und als Tunnel eingerichtet ist.

**Bridge:** Zeigt die Konfiguration der Bridges auf dem Router an. Dieser Punkt nur angezeigt, wenn die Verbindung als Bridge eingerichtet ist.

**Konfiguration:** Über diesen Punkt kann die beim Booten generierte Konfiguration der Verbindung angeschaut werden.

**Keymanagement:** Über diesen Punkt kann für diese Verbindung ein Schlüssel erzeugt und auch heruntergeladen werden. (siehe Abbildung 4.4) Ist kein Schlüssel vorhanden (beim ersten Start) wird automatisch einer generiert und angezeigt. Er kann über das Download-Symbol direkt heruntergeladen, oder mit copy/paste in eine Textdatei übertragen werden. Um einen neu generierten Schlüssel auf dem Router zu speichern, ist auf das Disketten-Symbol zu klicken. Ein solcher Speichervorgang kann mit einem Klick auf das Wiederherstellen Symbol rückgängig gemacht werden.

**Supportinformationen:** Hier werden alle Dinge angezeigt, die bei Problemen relevant sein könnten. Sie können diese Informationen dann beispielsweise auf Anfrage per copy&paste in einen Artikel der Newsgroup übertragen.

### 4.15.7. OpenVPN - Zusammenarbeit unterschiedlicher OpenVPN Versionen

Bei der Zusammenarbeit unterschiedlicher OpenVPN Versionen muss darauf geachtet werden, dass diese unterschiedliche Standardwerte für die Parameter einer Verbindung benutzen. Das betrifft insbesondere die MTU, Fragment und MSSFIX Einstellungen. Wenn die entsprechenden Werte nicht „zusammenpassen“, ist ein Verbindungsaufbau nicht möglich oder die Verbindung funktioniert zwar mit einem Pingbefehl, bricht aber beispielsweise bei der Benutzung von ssh zusammen. Typische Fehlermeldungen in einem solchen Fall sind z. B.:

```
FRAG_IN error flags=0xfa2a187b: FRAG_TEST not implemented
FRAG_IN error flags=0xfa287f34: spurious FRAG_WHOLE flags
```

Die entscheidenden Parameter für das Zustandekommen einer Verbindung sind folgende Einstellungen:

**OPENVPN\_x\_TUN\_MTU** Der MTU Wert des TUN Geräte war bei OpenVPN 1.x auf 1300 eingestellt. Ab OpenVPN 2.0 wird 1500 als Standardwert angenommen.

**OPENVPN\_x\_LINK\_MTU** Die Bytegröße der Verbindung der beiden OpenVPN Daemons. Dieser Standardwert ist abhängig von der verwendeten OpenVPN Version und des Betriebssystems.

**OPENVPN\_x\_FRAGMENT** Datenpakete (egal ob UDP oder TCP), deren Größe über der Fragmentgrenze liegt, werden auf Datenpakete aufgeteilt, die nicht größer sind als die unter OPENVPN\_x\_FRAGMENT angegebene Bytegröße.

**OPENVPN\_x\_MSSFIX** Damit TCP Verbindungen, die über das VPN Daten austauschen, nach Möglichkeit die Datenpakete nicht fragmentieren müssen, kann hier eine gewünschte maximale Größe der TCP Datenpakete vorgegeben werden. An diese Vorgabe halten sich dann aktuelle Betriebssysteme und ein aufwendiges Fragmentieren der Datenpakete ist nicht notwendig.

Die unterschiedlichen OpenVPN Versionen benutzen folgende Werte als Standardwerte. Diese Werte müssen Sie beachten, wenn Sie mit OpenVPN Versionen Kontakt aufnehmen wollen, die nicht auf einem fli4l-Router laufen. Die Standardwerte auf dem fli4l-Router sind in der zweiten Tabelle aufgeführt.

OpenVPN Version/Option	1.xx	2.00
OPENVPN_x_TUN_MTU	1300	1500
OPENVPN_x_TUN_MTU_EXTRA	unbekannt	32
OPENVPN_x_FRAGMENT	unbekannt	nicht konfiguriert
OPENVPN_x_MSSFIX	nicht konfiguriert	1450

Tabelle 4.11.: Unterschiedliche MTU Parameter der unterschiedlichen OpenVPN Versionen.

fli4l Version/Option	bis einschließlich 2.1.8	ab 2.1.9
OPENVPN_x_TUN_MTU	1300	1500
OPENVPN_x_TUN_MTU_EXTRA	64	32
OPENVPN_x_FRAGMENT	nicht konfiguriert	1300
OPENVPN_x_MSSFIX	nicht konfiguriert	1300

Tabelle 4.12.: Unterschiedliche MTU Parameter der fli4l-Router Versionen.

Aufgrund dieser unterschiedlichen Einstellungen, sollten Sie die für Ihr Netzwerk passenden Standardwerte ermitteln und diese dann explizit in die config/openvpn.txt schreiben. Folgende Werte sind in den meisten Fällen gute Startwerte für die ersten Tests.

```
OPENVPN_DEFAULT_TUN_MTU='1500'
OPENVPN_DEFAULT_MSSFIX='1300'
OPENVPN_DEFAULT_FRAGMENT='1300'
```

Leider gibt es für fli4l Versionen vor 2.1.9 keine Möglichkeit den „tun-mtu“ Parameter direkt zu setzen. Allerdings läßt sich dieser Parameter indirekt über den OPENVPN\_x\_LINK\_MTU beeinflussen. Der tun-mtu Wert ist ca. 45 Bytes kleiner als der bei OPENVPN\_x\_LINK\_MTU angegebene Wert. Um den genauen Wert zu ermitteln, hilft nur ausprobieren.

#### 4.15.8. OpenVPN - Beispiele

Einige Beispiele verdeutlichen die Konfiguration des OpenVPN Paketes.

**Beispiel - Zwei Netze mit fli4l-Routern verbinden**

Im ersten Beispiel werden zwei fli4l-Router miteinander verbunden. Die Netzwerke hinter den fli4l-Routern sollen dabei Zugriff auf das jeweils andere Netzwerk erhalten. In diesem Beispiel wollen Peter und Maria ihre Netzwerke über ihre fli4l-Router miteinander verbinden. Peter benutzt als privates Netz 192.168.145.0/24 und als DynDNS Adresse 'peter.eisfair.net'. Bei Maria sieht es ähnlich aus, nur benutzt sie das Netzwerk 10.23.17.0/24 und als DynDNS Adresse 'maria.eisfair.net'. Da sich beide unbegrenzt vertrauen, erlauben sie sich gegenseitig den kompletten Zugriff auf ihre jeweiligen Netze.

OpenVPN Option	Peter	Maria
OPENVPN_1_NAME=	'maria'	'peter'
OPENVPN_1_REMOTE_HOST=	'maria.eisfair.net'	'peter.eisfair.net'
OPENVPN_1_REMOTE_PORT=	'10000'	'10001'
OPENVPN_1_LOCAL_PORT=	'10001'	'10000'
OPENVPN_1_SECRET=	'pema.secret'	'pema.secret'
OPENVPN_1_TYPE=	'tunnel'	'tunnel'
OPENVPN_1_REMOTE_VPN_IP=	'192.168.200.202'	'192.168.200.193'
OPENVPN_1_LOCAL_VPN_IP=	'192.168.200.193'	'192.168.200.202'
OPENVPN_1_ROUTE_N=	'1'	'1'
OPENVPN_1_ROUTE_1=	'10.23.17.0/24'	'192.168.145.0/24'
OPENVPN_1_PF_INPUT_N=	'1'	'1'
OPENVPN_1_PF_INPUT_1=	'ACCEPT'	'ACCEPT'
OPENVPN_1_PF_FORWARD_N=	'1'	'1'
OPENVPN_1_PF_FORWARD_1=	'ACCEPT'	'ACCEPT'

Tabelle 4.13.: OpenVPN Konfiguration mit 2 fli4l-Routern

**Beispiel - Zwei Netze mit einer Bridge verbinden**

Im nächsten Beispiel wird eine Bridge über eine Funkverbindung aufgebaut. Bei einer Bridge kann der Paketfilter nicht sinnvoll konfiguriert werden, da dort nur Ethernetframes weitergeleitet werden, aber nicht unbedingt IP-Pakete. Bitte immer daran denken, dass bei einer Bridgekonfiguration ein gemeinsames Netz benutzt werden muss. Und es dürfen keine IP-Adressen doppelt vergeben werden.

OpenVPN Option	Peter	Maria
OPENVPN_2_NAME	'bridge'	'bridge'
OPENVPN_2_REMOTE_HOST	'10.1.0.1'	'10.2.0.1'
OPENVPN_2_REMOTE_PORT	'10005'	'10006'
OPENVPN_2_LOCAL_HOST	'10.2.0.1'	'10.1.0.1'
OPENVPN_2_LOCAL_PORT	'10006'	'10005'
OPENVPN_2_FLOAT	'no'	'no'
OPENVPN_2_RESTART	'never'	'never'
OPENVPN_2_SECRET	'bridge.secret'	'bridge.secret'
OPENVPN_2_TYPE	'bridge'	'bridge'
OPENVPN_2_BRIDGE	'pema-br'	'pema-br'

Tabelle 4.14.: OpenVPN Konfiguration mit 2 fli4l-Routern deren Netzwerk über eine Funkverbindung gebrückt wird.

Zusätzlich zu den Angaben für OpenVPN muss natürlich noch eine Bridge in `advanced_networking` konfiguriert werden und die `base.txt` so angepaßt werden, dass dort die Bridge

#### 4. Pakete

und nicht eth0 als Netzwerkdevice für das interne Netzwerk benutzt wird. Hier nochmal die relevanten Auszüge aus der Konfiguration von advanced\_networking und base.

advanced_networking Option	Peter	Maria
OPT_BRIDGE_DEV	'yes'	'yes'
BRIDGE_DEV_BOOTDELAY	'no'	'no'
BRIDGE_DEV_N	'1'	'1'
BRIDGE_DEV_1_NAME	'pema-br'	'pema-br'
BRIDGE_DEV_1_DEVNAME	'br0'	'br0'
BRIDGE_DEV_1_DEV_N	'1'	'1'
BRIDGE_DEV_1_DEV_1_DEV	'eth0'	'eth0'

Tabelle 4.15.: OpenVPN Konfiguration mit 2 fli4l-Routern deren Netzwerk über eine Funkverbindung gebrückt wird. Die Konfiguration der Bridge in advanced\_networking.

base Option	Peter	Maria
IP_NET_N	'1'	'1'
IP_NET_1	'192.168.193.254/24'	'192.168.193.1/24'
IP_NET_1_DEV	'br0'	'br0'

Tabelle 4.16.: OpenVPN Konfiguration mit 2 fli4l-Routern deren Netzwerk über eine Funkverbindung gebrückt wird. Die Konfiguration der Bridge in der Basiskonfiguration (base.txt).

#### Beispiel - Zugriff für einen Roadwarrior konfigurieren

Bei diesem Beispiel (Roadwarrior) wird über ein Notebook mit Windows XP und einem GPRS Zugang der Zugang zu dem LAN hinter dem fli4l-Router ermöglicht. Dazu wird auf dem Windows XP Notebook OpenVPN installiert und die entsprechende \*.ovpn Datei angepaßt. Leider ist der tun/tap Treiber unter Windows nicht ganz so flexibel wie sein Unix Gegenstück. Daher müssen die Point-to-Pointadressen für die VPN IP-Adressen in einem 255.255.255.252 (oder /30) Netz liegen. Wenn der Roadwarrior nur auf Dienste im LAN hinter und auf dem fli4l-Router zugreifen soll und nicht selber angesprochen werden muss, ist die Angabe einer Route auf der fli4l Seite nicht notwendig. Der Roadwarrior kann bei Bedarf über seine virtuelle IP-Adresse (OPENVPN\_3\_REMOTE\_VPN\_IP) angesprochen werden. Wenn der Roadwarrior über eine feste IP-Adresse verfügt, könnte man auch alternativ eine Hostroute eintragen. Wenn der Roadwarrior z.B. die feste IP-Adresse 192.168.33.33 hat, könnte man folgendes noch in die fli4l openvpn.txt Konfigurationsdatei einfügen:

```
OPENVPN_3_ROUTE_N='1'
OPENVPN_3_ROUTE_1='192.168.33.33/32'
```

Mit der Paketfilterkonfiguration, die hier im Beispiel gezeigt wird erlauben wir wieder die komplette Kommunikation in beide Richtungen. Nur auf den fli4l-Router direkt kann der Roadwarrior nicht zugreifen. Das wäre z.B. notwendig, wenn der Roadwarrior den DNS Server auf dem fli4l-Router benutzen soll.

```
OPENVPN_3_PF_FORWARD_N='1'
OPENVPN_3_PF_FORWARD_1='ACCEPT'
```

#### 4. Pakete

Soll der Zugriff vom Roadwarrior auf den internen DNS Server auf dem fli4l-Router erlaubt werden, muss noch folgendes zur fli4l Konfiguration dazugeschrieben werden:

```
OPENVPN_3_PF_INPUT_N='1'
OPENVPN_3_PF_INPUT_1='if:VPNDEV:any tmpl:dns ACCEPT'
```

OpenVPN Option fli4l-Router	roadwarrior
OPENVPN_3_NAME='roadwarrior'	remote peter.eisfair.net
OPENVPN_3_LOCAL_PORT='10011'	rport 10011
OPENVPN_3_SECRET='roadwarrior.secret'	secret roadwarrior.secret
OPENVPN_3_TYPE='tunnel'	dev tun
OPENVPN_3_REMOTE_VPN_IP='192.168.200.238'	
OPENVPN_3_LOCAL_VPN_IP='192.168.200.237'	ifconfig 192.168.200.238 192.168.200.237
OPENVPN_3_ROUTE_N='0'	
OPENVPN_3_PF_FORWARD_N='1'	
OPENVPN_3_PF_FORWARD_1='ACCEPT'	
	route 192.168.145.0 255.255.255.0
	comp-lzo
	persist-tun
	persist-key
	ping-timer-rem
	ping-restart 60
	proto udp4
	tun-mtu 1500
	fragment 1300
	mssfix

Tabelle 4.17.: OpenVPN Konfiguration mit einem Windowsrechner über GPRS.

#### Beispiel - WLAN Verbindung absichern

In diesem Beispiel wird eine WLAN Verbindung mit Hilfe von OpenVPN abgesichert. Es wird davon ausgegangen, dass im fli4l-Router sowohl eine LAN als auch eine WLAN Karte verwendet wird, oder ein Accesspoint an einer zusätzlichen Netzwerkkarte im fli4l angeschlossen ist. Ziel soll es sein, dass ein WLAN Client ohne VPN-Verbindung lediglich Zugriff auf den VPN Port des fli4l-Routers hat. Erst nach dem erfolgreichen Verbinden mit OpenVPN, soll uneingeschränkter Austausch mit dem Kabelgebundenen LAN möglich sein. Es müssen dafür auch Änderungen am DNSMASQ DHCP Server durchgeführt werden. Außerdem wird das advanced\_networking Paket benötigt. Einstellungen in base.txt: IP\_NET\_1 ist dabei das kabelgebundene LAN und IP\_NET\_2 das WLAN.

```
IP_NET_N='2'
IP_NET_1='192.168.3.254/24'
IP_NET_1_DEV='br0'
IP_NET_2='192.168.4.254/24'
IP_NET_2_DEV='eth2'
```

Die DHCP-Range ist nach Belieben einzustellen. Für IP\_NET\_2 sind aber unbedingt folgende Einstellungen hinzuzufügen:

```
DHCP_RANGE_2_DNS_SERVER1='none'
DHCP_RANGE_2_NTP_SERVER='none'
DHCP_RANGE_2_GATEWAY='none'
```

Einstellung in advanced\_networking.txt:

```

OPT_BRIDGE_DEV='yes'
BRIDGE_DEV_BOOTDELAY='yes'
BRIDGE_DEV_N='1'
BRIDGE_DEV_1_NAME='br'
BRIDGE_DEV_1_DEVNAME='br0'
BRIDGE_DEV_1_DEV_N='1'
BRIDGE_DEV_1_DEV_1_DEV='eth0'

```

OpenVPN Option Router	WLAN-Client
OPENVPN_4_NAME='wlan1'	
OPENVPN_4_LOCAL_HOST='192.168.4.254'	remote 192.168.4.254
OPENVPN_4_LOCAL_PORT='20001'	rport 20001
OPENVPN_4_SECRET='wlan1.secret'	secret wlan1.secret
OPENVPN_4_TYPE='bridge'	dev tap
OPENVPN_4_BRIDGE='br'	
OPENVPN_4_RESTART='never'	
OPENVPN_4_MUTE_REPLAY_WARNINGS='yes'	
	comp-lzo
	persist-tun
	persist-key
	ping-timer-rem
	ping-restart 60
	proto udp4
	tun-mtu 1500
	fragment 1300
	mssfix

Tabelle 4.18.: OpenVPN Absicherung eines WLAN.

#### 4.15.9. Weiterführende Links zum Thema OpenVPN

Abschliessend noch einige Links, die sich mit der Konfiguration von OpenVPN beschäftigen:

<http://openvpn.net>

<http://de.wikipedia.org/wiki/OpenVPN>

<http://openvpn.se/>

<http://arnowelzel.de/wiki/de/fli4l/openvpn>

<http://wiki.freifunk.net/OpenVPN>

<http://w3.linux-magazine.com/issue/24/Charly.pdf>

[http://w3.linux-magazine.com/issue/25/WirelessLAN\\_Intro.pdf](http://w3.linux-magazine.com/issue/25/WirelessLAN_Intro.pdf)

<http://w3.linux-magazine.com/issue/25/OpenVPN.pdf>

## 4.16. PCMCIA - PC-Card Unterstützung

### 4.16.1. PCMCIA-Treiber

fli4l kann auch mit PCMCIA-Karten zusammenarbeiten. Bei `OPT_PCMCIA='yes'` werden die entsprechenden Basis-Treiber installiert. Welche konkreten Kartentreiber verwendet werden sollen, wird z.B. über `NET_DRV_x` (Seite 39) eingestellt.

**PCMCIA\_PCIC** - PCMCIA Socket-Driver



Es kann dabei gewählt werden: 'i82365' oder 'tcic' für PCMCIA Bridges, sowie 'yenta\_socket' und 'i82092' für Cardbus Bridges.

Standard-Einstellung: PCMCIA\_PCIC='i82365'

#### **PCMCIA\_PCIC\_OPTS** - Optionen für den PCMCIA Socket-Driver

Standard-Einstellung: PCMCIA\_PCIC\_OPTS=""

Mögliche Einstellungen: poll\_interval=n n in je 10 Millisekunden - Sinnvoller Wert: 1000  
Stellt das Abfrageintervall für Kartenwechsel ein irq\_list=x,y,z,... Eine Liste der zu verwendenden Interrupts

**PCMCIA\_MISC\_N PCMCIA\_MISC\_x** Anzahl der zusätzlich zu ladenden PCMCIA-Module: serial\_cs für Modems und Combo-Karten parport\_cs Druckerschnittstellen

### 4.17. PPP - Unterstützung für das Point-to-Point-Protokoll

Mit Hilfe dieses Pakets kann der Router Verbindungen zu anderen Rechnern aufbauen, welche die PPP-Protokollfamilie als zugrunde liegendes Layer-2-Protokoll nutzen und PPP für die Aushandlung von IP-Adressen, Kompression, Verschlüsselung etc. verwenden. Die meisten Internet-Anbindungen in Deutschland nutzen PPP auf die eine oder andere Art. Wenn Sie einen Internet-Zugang via DSL, ISDN oder UMTS nutzen, benötigen Sie aller Voraussicht nach dieses Paket.

Dieses Paket bringt zum einen generelle Unterstützung für PPP mit. Zum anderen werden mit dem Paket gleich drei spezielle PPP-Module ("bundle", "serial" und "serial-server") aktiviert, mit denen PPP-Verbindungen gepündelt (PPP-Typ "bundle") oder ohne Modem über die serielle Schnittstelle mit Hilfe eines so genannten Null-Modem-Kabels<sup>8</sup> (PPP-Typen "serial" und "serial-server") genutzt werden können. Im Folgenden werden sowohl die allgemeinen Einstellungen für alle PPP-Circuit-Typen erläutert als auch die speziellen Einstellungen für die serielle Anbindung.

#### 4.17.1. Circuits vom Typ "ppp"

Ein Circuit vom Typ "ppp" baut eine Verbindung zwischen zwei Rechnern mit Hilfe des Point-to-Point-Protokolls (PPP)<sup>9</sup> auf. PPP ist ein recht komplexes Protokoll, mehr eine Protokollfamilie, und erlaubt eine Aushandlung von u. a. der zu verwendenden IP-Adressen, Kompression und/oder Verschlüsselung. Auch können mehrere PPP-Verbindungen zum selben Zielrechner ("Peer" genannt) gebündelt werden (MP).<sup>10</sup>

Das ppp-Paket bringt die nötige allgemeine Infrastruktur für PPP-Verbindungen mit. Diese wird über die folgende Variable eingebunden und aktiviert:

**OPT\_PPP** Diese Variable aktiviert den PPP-Dämon, der für alle PPP-Verbindungen notwendig ist.

Standard-Einstellung: OPT\_PPP='no'

Beispiel: OPT\_PPP='yes'

---

<sup>8</sup>Die Anschluss-Belegung ist im Anhang der Dokumentation des base-Pakets beschrieben.

<sup>9</sup>siehe RFC 1661

<sup>10</sup>"Multilink PPP", siehe RFC 1990 und den Abschnitt [Multilink PPP](#) (Seite 235)

#### 4. Pakete

Zusätzlich werden spezielle *PPP-Module* benötigt, die spezifisch für den jeweiligen Typ von Verbindung sind. Die folgende Tabelle listet die zugehörigen fli4l-Pakete samt Typ und Beschreibung auf.

PPP-Typ	Paket	OPT	Beschreibung
bundle	ppp (dieses Paket)	OPT_MULTILINK_PPP	Mit Hilfe von bundle-Circuits ist es möglich, PPP-Kanäle zu bündeln. Mehr dazu steht im Abschnitt <a href="#">Multilink PPP</a> (Seite 235).
serial	ppp (dieses Paket)	OPT_PPP_SERIAL	Mit Hilfe von serial-Circuits ist eine Verbindung zu einem anderen Rechner über ein seriell-Null-Modem-Kabel möglich.
ethernet	pppoe	OPT_PPP_ETHERNET	Mit Hilfe von ethernet-Circuits ist eine DSL-Einwahl ins Internet über PPPoE <sup>11</sup> möglich. Dabei ist der Router über eine normale Ethernet-Netzanbindung mit einem DSL-Modem verbunden, das dann die physikalische Einwahl durchführt.
dslmodem	dslmodem	OPT_PPP_DSLMODEM	Mit Hilfe von dslmodem-Circuits ist eine DSL-Einwahl ins Internet über ein im fli4l integriertes DSL-Modem möglich. Dabei ist der Router direkt mit dem DSL-Splitter verbunden. Momentan wird nur der Fritz!DSL-Adapter der Firma AVM unterstützt.
pptp	vpn	OPT_PPP_PPTP	Mit Hilfe von pptp-Circuits ist eine DSL-Einwahl ins Internet über PPTP <sup>12</sup> möglich. Dabei ist der Router über eine normale Ethernet-Netzanbindung mit einem DSL-Modem verbunden, das dann die physikalische Einwahl durchführt. Abgesehen von der Internet-Einwahl können pptp-Circuits auch für VPN-Tunnel eingesetzt werden, wobei auf Grund von Sicherheitsproblemen bei der Authentifizierung von ihrem Gebrauch abgeraten werden muss.
isdn	isdn	OPT_ISDN	Mit Hilfe von isdn-Circuits ist eine ISDN-Einwahl ins Internet über das HDLC-Protokoll <sup>13</sup> möglich. Dabei ist der Router mit Hilfe eines ISDN-Adapters mit einem NTBA verbunden. Die physikalische Einwahl wird von dem ISDN-Adapter durchgeführt.

<sup>11</sup>“Point-to-Point Protocol over Ethernet”, siehe RFC 2516

<sup>12</sup>“Point-to-Point Tunneling Protocol”, siehe RFC 2637

<sup>13</sup>“High-level data link control”, siehe RFC 1618

PPP-Typ	Paket	OPT	Beschreibung
umts	umts	OPT_UMTS	Mit Hilfe von umts-Circuits ist eine Einwahl ins Internet via UMTS oder LTE, also über eine geeignete Funkverbindung, möglich. Ein spezielles Funkmodem, das in der Regel als USB-Stick vorliegt, stellt die physikalische Anbindung her.
modem	modem	OPT_MODEM	Mit Hilfe von modem-Circuits ist eine Einwahl ins Internet über eine serielle Leitung möglich. Dabei stellt ein analoges Modem die physikalische Anbindung her.

Tabelle 4.19.: Verfügbare PPP-Typen

### Allgemeine PPP-Konfigurationsvariablen

Neben den allgemeinen Circuit-Variablen sind Angaben über die folgenden Variablen nötig:

**CIRC\_x\_PPP\_TYPE** Jeder ppp-Circuit hat einen Typ. Dieser Typ bestimmt, wie das Wählen und Auflegen eines ppp-Circuits konkret funktioniert.

Es sind immer nur die Typen der aktivierten Pakete verfügbar. Wenn Sie also z. B. einen PPP-over-Ethernet-Circuit (PPP-Typ "ethernet") verwenden möchten, dann müssen Sie das Paket `pppoe` herunterladen und PPP/ethernet-Circuits mit `OPT_PPP_ETHERNET='yes'` aktivieren. Andernfalls bekommen Sie bei der Verwendung des Typs "ethernet" beim Bauen der Installationsarchive eine Fehlermeldung.

Beispiel: `CIRC_1_PPP_TYPE='ethernet'`

**CIRC\_x\_PPP\_MTU** Mit dieser optionalen Variable kann die Größe der so genannten *MTU* (Maximum Transmission Unit) in Bytes eingestellt werden. Normalerweise beträgt die MTU 1492 Bytes, dies ist gleichzeitig die größtmögliche Angabe. Diese Einstellung sollte nur in Sonderfällen geändert werden!

Standard-Einstellung: je nach PPP-Typ

Beispiel: `CIRC_1_PPP_MTU='1488'`

**CIRC\_x\_PPP\_MRU** Mit dieser optionalen Variable kann die Größe der so genannten *MRU* (Maximum Receive Unit) in Bytes eingestellt werden. Normalerweise beträgt die MRU 1492 Bytes, dies ist gleichzeitig die größtmögliche Angabe. Diese Einstellung sollte nur in Sonderfällen geändert werden!

Standard-Einstellung: je nach PPP-Typ

Beispiel: `CIRC_1_PPP_MRU='1488'`

**CIRC\_x\_PPP\_NF\_MSS** Bei manchen Providern treten Effekte folgender Art auf:

- der Webbrowser bekommt eine Verbindung, macht aber danach nichts mehr
- eine kleine E-Mail kann verschickt werden, eine große E-Mail nicht
- ssh funktioniert, scp hängt nach dem initialen Verbindungsaufbau

Um diese Probleme zu umgehen, manipuliert fli4l standardmäßig die MTU. In einigen Fällen reicht das allerdings nicht, daher gestattet fli4l explizit das Setzen der MSS (Message Segment Size) für TCP-Verbindungen auf einen vom Provider vorgegebenen Wert. Falls der Provider nichts vorgibt, ist 1412 ein guter Startwert zum Probieren; falls er die MTU vorgibt, sind hier 40 Bytes (für IPv4-Verbindungen)<sup>14</sup> bzw. 60 Bytes (falls auch IPv6 genutzt werden soll)<sup>15</sup> weniger einzutragen.

Fehlt diese Variable oder wird sie leer gelassen, wird die MSS automatisch vom Linux-Kern aus der PMTU errechnet.<sup>16</sup>

Beispiel: `CIRC_1_PPP_NF_MSS='1412'`

**CIRC\_x\_PPP\_LOCALIP** Diese Variable legt die zu verwendende IPv4-Adresse auf Client-Seite für die PPP-Verbindung fest. Wird diese Variable weggelassen, wird eine temporäre IPv4-Adresse aus dem Adress-Bereich 169.254.0.0/16 genommen und gleichzeitig dem Peer signalisiert, dass man “offen für Vorschläge” ist, d.h. der Peer kann eine alternative IPv4-Adresse für unsere Seite der Verbindung vorschlagen. Dies ist z.B. bei Internet-Anbindungen üblich.

Beispiel: `CIRC_1_PPP_LOCALIP='192.168.11.22'`

**CIRC\_x\_PPP\_REMOTEIP** Diese Variable legt die zu verwendende IPv4-Adresse auf Peer-Seite für die PPP-Verbindung fest. Wird diese Variable weggelassen, wird eine temporäre IPv4-Adresse aus dem Adress-Bereich 169.254.0.0/16 genommen und gleichzeitig dem Peer signalisiert, dass man “offen für Vorschläge” ist, d.h. der Peer kann eine alternative IPv4-Adresse für seine Seite der Verbindung vorschlagen. Dies ist z.B. bei Internet-Anbindungen üblich.

Beispiel: `CIRC_1_PPP_REMOTEIP='192.168.11.23'`

**CIRC\_x\_PPP\_LOCALIP6** Diese Variable legt das Suffix der zu verwendenden IPv6-Adresse auf Client-Seite für die PPP-Verbindung fest. Wird diese Variable weggelassen, wird `::2` genommen. In jedem Fall wird dem Peer signalisiert, dass man “offen für Vorschläge” ist, d.h. der Peer kann eine alternative IPv6-Adresse für unsere Seite der Verbindung vorschlagen. Dies ist z.B. bei Internet-Anbindungen üblich.

Beispiel: `CIRC_1_PPP_LOCALIP6='::2'`

**CIRC\_x\_PPP\_REMOTEIP6** Diese Variable legt die zu verwendende IPv6-Adresse auf Peer-Seite für die PPP-Verbindung fest. Wird diese Variable weggelassen, wird `::1` genommen. In jedem Fall wird dem Peer signalisiert, dass man “offen für Vorschläge” ist, d.h. der Peer kann eine alternative IPv4-Adresse für seine Seite der Verbindung vorschlagen. Dies ist z.B. bei Internet-Anbindungen üblich.

Beispiel: `CIRC_1_PPP_REMOTEIP6='::1'`

**CIRC\_x\_PPP\_FILTER** Der fli4l legt automatisch auf, wenn während der über den Hangup-Timeout angegebenen Zeit keine Daten über die PPP-Schnittstelle gehen. Leider wertet

<sup>14</sup>siehe RFC 879

<sup>15</sup>siehe RFC 2460

<sup>16</sup>Die PMTU oder Pfad-MTU (“Path MTU”) ist die MTU für den gesamten Netzwerkpfad zwischen Sender und Empfänger und berechnet sich aus dem Minimum aller MTUs auf dem Weg zwischen Sender und Empfänger.

der Linux-Kern auch Datentransfers mit, die von außen kommen, z. B. durch Verbindungsversuche eines P2P-Clients wie eDonkey. Da man heutzutage eigentlich permanent von anderen kontaktiert wird, kann es passieren, dass fli4l die DSL-Verbindung nie beendet.

Hier hilft die Option `CIRC_x_PPP_FILTER`. Setzt man die Variable auf 'yes', wird nur noch Verkehr gewertet, der von der eigenen Maschine generiert wird, und von außen eingehende Daten werden komplett ignoriert. Da von draußen hereinkommender Datenverkehr in der Regel dazu führt, dass der Router oder dahinter liegende Rechner reagieren, indem sie z. B. Verbindungswünsche ablehnen, werden zusätzlich noch einige hinausgehende Pakete ignoriert. <sup>17</sup>

Standard-Einstellung: `CIRC_x_PPP_FILTER='no'`

Beispiel: `CIRC_1_PPP_FILTER='yes'`

**CIRC\_x\_PPP\_FILTER\_EXPR** Hier steht der zu nutzende Filter, wenn `CIRC_x_PPP_FILTER` auf 'yes' gesetzt ist. Ist die Variable undefiniert oder leer, wird der Standard-Filter genutzt. Dieser lautet:

```
outbound and not icmp[0] != 8 and not tcp[13] & 4 != 0
```

Zu beachten ist, dass der Standard-Ausdruck oder der hier angegebene Ausdruck (je nachdem) unter Umständen erweitert wird, wenn andere OPTs aktiviert werden. So verhindert das IPv6-OPT, dass bestimmte IPv6-Multicast-Pakete, die vom Linux-Kern über jede IPv6-fähige Schnittstelle versandt werden, die Verbindung aufrecht erhalten, und das Chrony-OPT erweitert den Ausdruck dergestalt, dass Zeitabfragen für die Messung der Netzaktivität ignoriert werden, damit die regelmäßige Zeitsynchronisation via NTP nicht zu einer Dauereinwahl führt. Der hier angegebene Ausdruck kann sich somit von dem letztlich verwendeten unterscheiden.

Standard-Einstellung: `CIRC_x_PPP_FILTER_EXPR=''`

Beispiel: `CIRC_1_PPP_FILTER_EXPR='outbound and tcp dst port 80'`

Dieser (nicht unbedingt praxistaugliche) Ausdruck berücksichtigt nur ausgehende HTTP-Verbindungen (TCP-Verbindungen zu Port 80). Alle anderen Datenpakete fließen in die Bewertung der Netzaktivität nicht mit ein.

### Authentifizierung

PPP ermöglicht es, dass die Rechner auf beiden Seiten einer Verbindung sich gegenseitig authentifizieren, d.h. mit Hilfe einer jeweils vom anderen Rechner akzeptierten Kombination eines Benutzernamens und eines Passworts ausweisen. Die im Folgenden erläuterten Einstellungen erlauben es, die PPP-Authentifizierung wunschgemäß zu konfigurieren.

### CIRC\_x\_PPP\_USERID

---

<sup>17</sup>Wie das genau funktioniert, kann man unter <http://www.fli4l.de/hilfe/howtos/basteleien/hangup-problem-loesen/> und <http://web.archive.org/web/20061107225118/http://www.linux-bayreuth.de/dcforum/DCForumID2/46.html> nachlesen.

**CIRC\_x\_PPP\_PASSWORD** Hier sind Benutzerkennung und Passwort für den jeweils benutzten PPP-Peer (das ist i. d. R. der Internet-Provider) anzugeben. **CIRC\_x\_PPP\_USERID** enthält die Benutzerkennung, **CIRC\_x\_PPP\_PASSWORD** das Passwort.

Für einen T-Online-Zugang ist Folgendes zu beachten:

Die Benutzerkennung **AAAAAAAAAAAAATTTTTTTTTTTTMMM@t-online.de** setzt sich aus der zwölfstelligen Anschlusskennung **AAAAAA...**, der T-Online-Nummer **TTTTTT...**, der vierstelligen Mitbenutzernummer **MMM** und dem Suffix **@t-online.de** zusammen. Hinter der T-Online-Nummer muss ein **#** angegeben werden, wenn deren Länge kürzer als zwölf Zeichen ist.

Sollte dies in Einzelfällen nicht zum Erfolg führen (offenbar abhängig von der Vermittlungsstelle), muss zusätzlich zwischen der Anschlusskennung und der T-Online-Nummer ein weiteres **#**-Zeichen eingefügt werden.

Ansonsten (T-Online-Nummer ist zwölfstellig) sind keine **#**-Zeichen anzugeben.

Beispiel:

```
CIRC_1_PPP_USERID='111111111111222222#0001@t-online.de'  
CIRC_1_PPP_PASSWORD='12345678'
```

Informationen über Benutzerkennungen bei anderen Providern finden sich in der FAQ ([http://extern.fli4l.de/fli4l\\_faqengine/faq.php?list=category&catnr=3&prog=1](http://extern.fli4l.de/fli4l_faqengine/faq.php?list=category&catnr=3&prog=1)).

**CIRC\_x\_PPP\_PEER\_AUTH** Mit dieser optionalen Variable kann der PPP-Peer aufgefordert werden, sich zu authentifizieren. Dazu muss er einen gültigen Benutzernamen und ein gültiges Passwort übermitteln. Welche Benutzername/Passwort-Kombinationen für welche Circuits gültig sind, wird über das **OPT\_PPP\_PEERS** eingestellt. Generell ist dies eher für PPP-Circuits auf Server-Seite interessant.

Standard-Einstellung: **CIRC\_x\_PPP\_PEER\_AUTH='no'**

Beispiel: **CIRC\_1\_PPP\_PEER\_AUTH='yes'**

#### TCP/IP-Kompression

PPP bietet die Möglichkeit, für TCP/IPv4-Verbindungen die Van Jacobson-Header-Komprimierung nach RFC 1144 zu aktivieren und somit die effektive Bandbreite zu erhöhen. Dies ist vor allem bei eher langsamer physikalischer Anbindung (serielle Leitung, ISDN) nützlich.

Generell gilt, dass diese Form der Kompression dazu führt, dass im Falle verloren gegangener Pakete es etwas dauert, bis der Fehler bemerkt und auf beiden Seiten entsprechende Korrekturmaßnahmen eingeleitet worden sind.

**CIRC\_x\_PPP\_VJ** Diese Variable aktiviert die Van Jacobson-Komprimierung für TCP/IPv4-Header.

Standard-Einstellung: **CIRC\_x\_PPP\_VJ='no'**

Beispiel: **CIRC\_1\_PPP\_VJ='yes'**

**CIRC\_x\_PPP\_VJCCOMP** Mit dieser Option kann man erreichen, dass trotz aktivierter Van Jacobson-Komprimierung (**CIRC\_x\_PPP\_VJ='yes'**) die Verbindungsnummer ("Connection ID") Teil eines jeden Pakets ist. Dies erreicht man durch **CIRC\_x\_PPP\_VJCCOMP='no'**,

ein Weglassen der Verbindungsnummer erreicht man durch `CIRC_x_PPP_VJCCOMP='yes'`. Das unbedingte Senden der Verbindungsnummer (`CIRC_x_PPP_VJCCOMP='no'`) kann dazu führen, dass im Falle verloren gegangener Pakete es nicht ganz so lange dauert, bis der Fehler bemerkt und auf beiden Seiten entsprechende Korrekturmaßnahmen eingeleitet worden sind.

Standard-Einstellung: `CIRC_x_PPP_VJCCOMP='no'`

Beispiel: `CIRC_1_PPP_VJCCOMP='yes'`

### PPP-Kompression

PPP bietet die Möglichkeit, unabhängig für jede Verbindungsrichtung das Komprimieren (Packen) von Paketen auszuhandeln. Dies wird über die folgenden Variablen konfiguriert. Das Aktivieren der `CIRC_x_PPP_COMP_y`-Variablen hat zur Folge, dass dem Verbindungspartner (Peer) angeboten wird, ihm die Pakete komprimiert zu schicken (was er verweigern kann, etwa wenn er die vorgeschlagene Kompression nicht versteht). Im Gegenzug führt das Aktivieren der `CIRC_x_PPP_DECOMP_y`-Variablen dazu, dass dem Peer mitgeteilt wird, dass man in der Lage ist, bestimmte komprimierte Pakete verarbeiten (d. h. entpacken) zu können. Es handelt sich in beiden Fällen jeweils um *Vorschläge*, die entsprechend zurückgewiesen werden können – man kann den Peer nicht dazu zwingen, die Pakete komprimiert zu verschicken oder komprimierte Pakete zu verarbeiten.

Generell ist das Entpacken effizienter zu realisieren als das Packen. Ist die Hardware des fli4l-Routers nicht sehr leistungsfähig, ist es somit u. U. zu empfehlen, höchstens das Entpacken anzubieten (`CIRC_x_PPP_DECOMP_y='yes'`) und das Packen nicht (`CIRC_x_PPP_COMP_y='no'`).

### CIRC\_x\_PPP\_COMP\_BSDCOMP

**CIRC\_x\_PPP\_DECOMP\_BSDCOMP** Diese Variablen aktivieren die Möglichkeit, Pakete vor dem Versenden an den Peer mit Hilfe des BSD-Kompressionsalgorithmus zu komprimieren (`CIRC_x_PPP_COMP_BSDCOMP='yes'`) bzw. entsprechend komprimierte Pakete vom Peer zu empfangen (`CIRC_x_PPP_DECOMP_BSDCOMP='yes'`).

Standard-Einstellung:

`CIRC_x_PPP_COMP_BSDCOMP='no'`

`CIRC_x_PPP_DECOMP_BSDCOMP='no'`

Beispiel:

`CIRC_1_PPP_COMP_BSDCOMP='yes'`

`CIRC_1_PPP_DECOMP_BSDCOMP='yes'`

### CIRC\_x\_PPP\_COMP\_BSDCOMP\_LEVEL

**CIRC\_x\_PPP\_DECOMP\_BSDCOMP\_LEVEL** Ist die BSD-Kompression mit Hilfe der Variablen `CIRC_x_PPP_COMP_BSDCOMP='yes'` bzw. `CIRC_x_PPP_DECOMP_BSDCOMP='yes'` aktiviert worden, kann mit Hilfe der Variablen `CIRC_x_PPP_COMP_BSDCOMP_LEVEL` bzw. `CIRC_x_PPP_DECOMP_BSDCOMP_LEVEL` die zu verwendende Kompressionsstufe konfiguriert werden. Diese Variablen erwarten einen Wert von 9 (schwächste Kompression, am schnellsten) bis 15 (stärkste Kompression, am langsamsten).

Diese Stufe ist jeweils als Vorschlag einer oberen Grenze zu sehen; der Peer kann eine schwächere Stufe aushandeln, falls er mit dem Vorschlag nicht einverstanden ist.

Standard-Einstellung:

```
CIRC_x_PPP_COMP_BSDCOMP_LEVEL='12'  
CIRC_x_PPP_DECOMP_BSDCOMP_LEVEL='12'
```

Beispiel (langsame Hardware, nur schwache Kompression möglich):

```
CIRC_1_PPP_COMP_BSDCOMP_LEVEL='9'  
CIRC_1_PPP_DECOMP_BSDCOMP_LEVEL='15'
```

#### **CIRC\_x\_PPP\_COMP\_DEFLATE**

**CIRC\_x\_PPP\_DECOMP\_DEFLATE** Diese Variablen aktivieren die Möglichkeit, Pakete vor dem Versenden an den Peer mit Hilfe des Deflate-Kompressionsalgorithmus zu komprimieren (`CIRC_x_PPP_COMP_DEFLATE='yes'`) bzw. entsprechend komprimierte Pakete vom Peer zu empfangen (`CIRC_x_PPP_DECOMP_DEFLATE='yes'`).

Standard-Einstellung:

```
CIRC_x_PPP_COMP_DEFLATE='no'  
CIRC_x_PPP_DECOMP_DEFLATE='no'
```

Beispiel:

```
CIRC_1_PPP_COMP_DEFLATE='yes'  
CIRC_1_PPP_DECOMP_DEFLATE='yes'
```

#### **CIRC\_x\_PPP\_COMP\_DEFLATE\_LEVEL**

**CIRC\_x\_PPP\_DECOMP\_DEFLATE\_LEVEL** Ist die Deflate-Kompression mit Hilfe der Variablen `CIRC_x_PPP_COMP_DEFLATE='yes'` bzw. `CIRC_x_PPP_DECOMP_DEFLATE='yes'` aktiviert worden, kann mit Hilfe der Variablen `CIRC_x_PPP_COMP_DEFLATE_LEVEL` bzw. `CIRC_x_PPP_DECOMP_DEFLATE_LEVEL` die zu verwendende Kompressionsstufe konfiguriert werden. Diese Variablen erwarten einen Wert von 9 (schwächste Kompression, am schnellsten) bis 15 (stärkste Kompression, am langsamsten).

Diese Stufe ist jeweils als Vorschlag einer oberen Grenze zu sehen; der Peer kann eine schwächere Stufe aushandeln, falls er mit dem Vorschlag nicht einverstanden ist.

Standard-Einstellung:

```
CIRC_x_PPP_COMP_DEFLATE_LEVEL='12'  
CIRC_x_PPP_DECOMP_DEFLATE_LEVEL='12'
```

Beispiel (langsame Hardware, nur schwache Kompression möglich):

```
CIRC_1_PPP_COMP_DEFLATE_LEVEL='9'  
CIRC_1_PPP_DECOMP_DEFLATE_LEVEL='15'
```

#### **CIRC\_x\_PPP\_COMP\_LZSCOMP**

**CIRC\_x\_PPP\_DECOMP\_LZSCOMP** Diese Variablen aktivieren die Möglichkeit, Pakete vor dem Versenden an den Peer mit Hilfe des Stac/HiFn-LZS-Kompressionsalgorithmus zu komprimieren (`CIRC_x_PPP_COMP_LZSCOMP='yes'`) bzw. entsprechend komprimierte Pakete vom Peer zu empfangen (`CIRC_x_PPP_DECOMP_LZSCOMP='yes'`).



#### 4. Pakete

Der Nutzung dieses Algorithmus ist lizenzrechtlich problematisch. Die Implementierung für das ISDN4Linux-Subsystem des Linux-Kerns enthält die folgende Passage:

```
The code is Copyleft 1998-2001 by Andre Beck under terms of the
GNU GPL. While the code is provided free and under GPL, it may infringe
patents Stac has applied for in the US and maybe other countries. Verify
that this is not the case in your country before using it. This code is a
private development related in no way whatsoever to my employer, written
in Germany where software patents are still considered bogus. This
situation might change any day due to EU law. Linux distributors who
supply this stuff shrink wrapped should reconsider doing this (not only
for isdn_lzscmp, but as well for isdn_bsdcomp, which is likely to
infringe on the infamous Unisys LZW patent) with their law departement.
[...]
```

```
Please check whether using this code constitutes a crime in your country.
While I just implemented a module that can source and sink the data
format described by Stac/HiFn in RFC1974, they claim to have US Patents
on practically every aspect of this format. Thus I assume that selling
this code violates these US Patents. As this code is
```

- a) Freeware under GPL and
- b) Developed in Germany

```
I hope I wont get any terror from the lawyers of the patent holders. I'm
sure that the availability of this code will actually help HiFn sales
because more users (the Linux community) will ask their ISPs for LZS
support on their NASes and these NASes will contain HiFn chips for that
purpose. Then again, after they claimed even deflate would be covered by
their patents and tried to sue Netscape for using deflate in the PNG code
of Mozilla, they are probably not on the planet for good will games.
We'll see.
```

Außerdem gibt es Probleme, wenn die Datenübertragung nicht sehr stabil ist und gelegentlich Pakete verloren gehen: Die dann nötige Resynchronisation der Zustände des Kompressors/Dekompressors reduziert die Übertragungsgeschwindigkeit derart, dass der Geschwindigkeitsgewinn u. U. gänzlich aufgefressen wird.

Man sollte den Algorithmus somit nur verwenden, wenn man muss, wenn der PPP-Peer also keinen anderen, frei verfügbaren Algorithmus anbietet bzw. versteht und man die Komprimierung gerne nutzen möchte (was sich vor allem bei eher langsamen Verbindungen wie ISDN merklich auf die Übertragungsgeschwindigkeit auswirkt). Ansonsten sollte man ausprobieren, ob mit eingeschalteter Kompression die Datenübertragung in den eigenen typischen Anwendungsfällen wirklich schneller ist.

Standard-Einstellung:

```
CIRC_x_PPP_COMP_LZSCOMP='no'
CIRC_x_PPP_DECOMP_LZSCOMP='no'
```

Beispiel:

```
CIRC_1_PPP_COMP_LZSCOMP='yes'
CIRC_1_PPP_DECOMP_LZSCOMP='yes'
```

### **CIRC\_x\_PPP\_COMP\_LZSCOMP\_NHIST**

**CIRC\_x\_PPP\_DECOMP\_LZSCOMP\_NHIST** Ist die Stac-LZS-Kompression mit Hilfe der Variablen `CIRC_x_PPP_COMP_LZSCOMP='yes'` bzw. `CIRC_x_PPP_DECOMP_LZSCOMP='yes'` aktiviert worden, kann mit Hilfe der Variablen `CIRC_x_PPP_COMP_LZSCOMP_NHIST` bzw. `CIRC_x_PPP_DECOMP_LZSCOMP_NHIST` eingestellt werden, wie viele verschiedene Historien verwendet werden sollen. Verschiedene Historien erlauben es, verschiedene TCP-Verbindungen unabhängig voneinander zu komprimieren. Aufgrund von Einschränkungen im Linux-Kern werden momentan jedoch nur zwei Einstellungen unterstützt: 0 (keine Historie) und 1 (eine Historie). Bei 0 wird jedes Paket individuell komprimiert. Das senkt den Kompressionsgewinn erheblich, erhöht jedoch die Robustheit, da ein Verlust eines Pakets sich nicht auf die anderen übertragenen Pakete auswirkt.

Dieser Wert ist jeweils als Vorschlag einer oberen Grenze zu sehen; der Peer kann weniger Historien aushandeln, falls er mit dem Vorschlag nicht einverstanden ist.

Standard-Einstellung:

```
CIRC_x_PPP_COMP_LZSCOMP_NHIST='1'
CIRC_x_PPP_DECOMP_LZSCOMP_NHIST='1'
```

Beispiel (hochgradig unzuverlässige Verbindung):

```
CIRC_1_PPP_COMP_LZSCOMP_NHIST='0'
CIRC_1_PPP_DECOMP_LZSCOMP_NHIST='0'
```

**PPP\_COMP\_LZSCOMP\_LEVEL** Diese globale, nicht Circuit-spezifische Variable gibt an, welche Stufe beim Stac/HiFn-LZS-Algorithmus für die Komprimierung von Paketen verwendet werden soll. Diese Variable erwartet einen Wert von 1 (schwächste Kompression, am schnellsten) bis 9 (stärkste Kompression, am langsamsten).

Diese Einstellung ist global, weil sie nicht Teil der Aushandlung der PPP-Verbindungseigenschaften ist und beim Laden des entsprechenden Kern-Moduls fest angegeben werden muss.

Stufe 9 ist nicht unbedingt für den produktiven Betrieb geeignet. Die Dokumentation besagt:

```
Try 9 only for fun, it is rather useless (compresses only 1 or 2%
better than 8, but a P100 facing that amount of brute force becomes
sluggish, jumping mouse etc) - just not worth the burned CPU (even
if you have a GHz oven).
```

Standard-Einstellung:

```
PPP_COMP_LZSCOMP_LEVEL='8'
```

Beispiel (langsame Hardware, nur schwache Kompression möglich):

```
PPP_COMP_LZSCOMP_LEVEL='1'
```

**CIRC\_x\_PPP\_COMP\_MPPE** Diese Variable aktiviert die Möglichkeit, Pakete vor dem Versenden an den Peer mit Hilfe des MPPE-Algorithmus zu komprimieren und zu verschlüsseln. Im Gegensatz zu den anderen Algorithmen gibt es keine separate Einstellung für die Pakete vom Peer zum fli4l-Router, weil MPPE immer symmetrisch ausgehandelt wird, d. h. dass MPPE entweder für beide Richtungen aktiv ist oder für keine.

MPPE wird vor allem in Zusammenhang mit PPTP-Tunneln genutzt. Für andere Einsatzzwecke sollte MPPE aufgrund bekannter kryptographischer Schwachstellen nicht verwendet werden.

Standard-Einstellung: `CIRC_x_PPP_COMP_MPPE='no'`

Beispiel: `CIRC_1_PPP_COMP_MPPE='yes'`

**CIRC\_x\_PPP\_COMP\_MPPE\_KEY\_LEN** Ist die MPPE-Verschlüsselung mit Hilfe der Variable `CIRC_x_PPP_COMP_MPPE='yes'` aktiviert, ist es u. U. nötig, die erlaubten Schlüssellängen einzustellen. Dies kann mit Hilfe der Variable `CIRC_x_PPP_COMP_MPPE_KEY_LEN` konfiguriert werden. Es gibt drei Möglichkeiten:

Wert	Bedeutung
40	Es soll ein 40-Bit-Schlüssel verwendet werden. Die Aushandlung eines 128-Bit-Schlüssels wird abgelehnt. ( <i>nicht empfohlen</i> )
128	Es soll ein 128-Bit-Schlüssel verwendet werden. Die Aushandlung eines 40-Bit-Schlüssels wird abgelehnt. ( <i>empfohlen</i> )
both	Es können sowohl 40-Bit- als auch 128-Bit-Schlüssel genutzt werden. ( <i>nicht empfohlen</i> )

Tabelle 4.20.: Mit `CIRC_x_PPP_COMP_MPPE_KEY_LEN` konfigurierbare MPPE-Schlüssellängen

Generell gilt: Je länger der Schlüssel, desto sicherer die Verschlüsselung. Wenn möglich, sollten somit immer 128-Bit-Schlüssel verwendet werden.

Standard-Einstellung:

`CIRC_x_PPP_COMP_MPPE_KEY_LEN='128'`

Beispiel (für die Nutzung eines Peers, der nur mit 40-Bit-Schlüsseln umgehen kann):

`CIRC_1_PPP_COMP_MPPE_KEY_LEN='40'`

#### 4.17.2. Multilink PPP: PPP-Circuits vom Typ “bundle”

PPP erlaubt es, mehrere Verbindungen zum selben Peer zu *bündeln*. Das bedeutet, dass mehrere unterschiedliche physische Verbindungen (z. B. ISDN-Kanäle oder Ethernet-Netzwerkverbindungen) logisch zu einer *einzigsten* Verbindung (“Bündel” genannt) zusammengefasst werden können. Somit handelt es sich bei Multilink PPP um eine Variante des BONDings.<sup>18</sup> Pakete, die über ein Multilink-Bündel transportiert werden, werden zuerst in einzelne Fragmente aufgeteilt. Diese Fragmente werden dann über die zum Bündel gehörenden PPP-Verbindungen

<sup>18</sup>BOND steht für “Bandwidth ON Demand” und bezeichnet eine Technik, bei der dynamisch – je nach Auslastung der (logischen) Verbindung – weitere physische Übertragungskanäle hinzugefügt oder bestehende entfernt werden, ohne dass die logische Verbindung etwas davon mitbekommt.

verschickt und auf der Gegenseite vom Peer wieder in der richtigen Reihenfolge zusammengebaut.<sup>19</sup> Bei genügend viel Datenverkehr werden alle Verbindungen im Bündel gleichmäßig ausgelastet, was zur Erhöhung der Übertragungsgeschwindigkeit führt, weil mehr Daten pro Zeiteinheit übertragen werden können.

Um Multilink PPP zu konfigurieren, muss ein so genanntes *PPP-Bündel* konfiguriert werden. Das ist ein spezieller PPP-Circuit vom Typ "bundle". Alle eigentlichen PPP-Kanäle, die gebündelt werden sollen, müssen dann dieses Bündel mit Hilfe der Variable `CIRC_x_BUNDLE` referenzieren. Dies funktioniert gleichermaßen auf Client- wie auf Server-Seite. Wird weiterhin die Dial-on-Demand-Funktionalität des `fl4l` für diesen Bündel-Circuit aktiviert (d.h. dass erst bei tatsächlich ausgehenden Netzwerkpaketen gewählt werden soll), muss einer dieser Circuits im Bündel als so genannter "Master" ausgezeichnet werden, der auf diese Pakete "horcht"; dies wird mit Hilfe der Variablen `CIRC_x_PPP_MASTER` vorgenommen.

Generell können die PPP-Kanäle eines PPP-Bündels beliebig hinzu- und herausgenommen werden: So lange auch nur ein Kanal im Bündel verbleibt, bleibt das gesamte Bündel intakt. Im Falle von Dial-on-Demand-Bündeln (siehe oben) ist die Situation etwas anders: Legt der Master-Circuit auf, so legen auch alle anderen Kanäle desselben Bündels auf.

Bei Multilink PPP muss man zum einen beachten, dass mehrere physisch *unabhängige* Übertragungskanäle genutzt werden (müssen). Dies bedeutet in der Regel, dass die Kosten sich entsprechend vervielfachen (wenn man z. B. mehrere ISDN-Verbindungen oder mehrere DSL-Verbindungen nutzt). Zum anderen müssen *beide* Verbindungspartner Multilink PPP unterstützen. Wenn der eigene Internet-Provider kein Multilink PPP anbietet, hat man also Pech... Typischerweise bieten Internet-Provider bei ISDN-Verbindungen Multilink PPP an, während dies bei DSL-Verbindungen die Seltenheit ist.

Multilink PPP ist aber natürlich nicht auf die Verbindung zum Internet-Provider beschränkt, sondern kann auch für andere Zwecke verwendet werden, etwa um lokale Netze übers Internet mit Hilfe mehrerer, unabhängiger Verbindungen performant zu verbinden. Wenn jedoch keine spezielle PPP-Funktionalität wie Kompression oder IP-Adress-Vergabe benötigt wird, ist im Falle von Ethernet-Verbindungen das von Linux angebotene Ethernet-Bonding effizienter, weil der Overhead des PPP-Protokolls entfällt.

Viele Einstellungen müssen für das gesamte PPP-Bündel identisch sein. Dies wird so realisiert, dass einige Einstellungen nur beim PPP-Bündel-Circuit konfiguriert werden (können) und die zugehörigen PPP-Kanäle diese übernehmen. Deswegen ist es erforderlich, dass der Bündel-Circuit *vor* den Circuits für die einzelnen PPP-Kanäle konfiguriert wird, d. h. einen niedrigeren Index besitzt. Die folgenden Einstellungen werden von den Kanälen übernommen bzw. haben nur auf den Bündel-Circuit Auswirkungen und dürfen folglich *nicht* für PPP-Kanäle separat konfiguriert werden:

- alles, was mit Netzwerk-Eigenschaften zu tun hat (Protokolle, Routen etc.):
  - `CIRC_x_NETS_IPV4_%`
  - `CIRC_x_NETS_IPV6_%`
  - `CIRC_x_PROTOCOLS`
  - `CIRC_x_USEPEERDNS`
  - `CIRC_x_PPP_NF_MSS`

---

<sup>19</sup>Die Anzahl der Fragmente sowie die Auswahl der Verbindungen erfolgt automatisch vom Linux-Kern und ist nicht beeinflussbar.

- Authentifizierung:
  - CIRC\_x\_PPP\_USERID
  - CIRC\_x\_PPP\_PASSWORD
  - CIRC\_x\_PPP\_PEER\_AUTH
- Paketfilter und Hangup-Timeout:
  - CIRC\_x\_HUP\_TIMEOUT
  - CIRC\_x\_PPP\_FILTER
- alle PPP-Kompressionseinstellungen<sup>20</sup>
- CIRC\_x\_PPP\_MRRU

Typische individuelle Einstellungen für einen PPP-Kanal sind die **MTU** (Seite 227) und die **MRU** (Seite 227), die für jede physische Verbindung separat konfiguriert werden (können) sowie Einstellungen, die den jeweiligen PPP-Typ betreffen (also z. B. die Netzwerk-Schnittstelle bei einer PPPoE-Verbindung) und somit ebenfalls für jede physische Verbindung unterschiedlich sind bzw. sein können.

Die Unterstützung für PPP-Bündel wird über die folgende Variable eingebunden und aktiviert:

**OPT\_MULTILINK\_PPP** Diese Variable aktiviert die PPP-Multilink-Unterstützung. Zusätzlich muss das **OPT\_BUNDLE** aus dem base-Paket aktiviert werden.

Standard-Einstellung: `OPT_MULTILINK_PPP='no'`

Beispiel:

```
OPT_BUNDLE='yes'
OPT_MULTILINK_PPP='yes'
```

Bei einem Bündel-Circuit kommen zu den allgemeinen Circuit- und PPP-Circuit-Variablen noch die folgenden hinzu, die spezifisch für PPP/bundle-Circuits sind:

**CIRC\_x\_PPP\_MASTER** Falls das PPP-Bündel für Dial-on-Demand konfiguriert ist (d.h. falls im Bündel `CIRC_x_HUP_TIMEOUT` größer null ist), dann wird mit Hilfe dieser Variable festgelegt, welcher PPP-Kanal zuerst aufgebaut wird. Dies ist nötig, weil nicht alle PPP-Kanäle gleichzeitig auf Netzwerkaktivität horchen können. Der Wert kann ein Bezeichner der Form `circ<Index>` oder der Name (`CIRC_Index_NAME='Name'`) des jeweiligen Circuits sein. Der referenzierte Circuit muss ein PPP-Circuit sein, der Teil dieses Bündels ist.

Bei Circuits, die sich sofort einwählen (`CIRC_x_HUP_TIMEOUT='0'`), wird diese Einstellung ignoriert.

Beispiel: `CIRC_1_PPP_MASTER='ppp-serial1'`

---

<sup>20</sup>Der verwendete PPP-Dämon unterstützt Kompression nur auf Bündel- und nicht auf Verbindungsebene.

**CIRC\_x\_PPP\_MRRU** Die MRRU ist die [MRU](#) (Seite 227) auf der Ebene des Multilink-Bündels. Sie sagt aus, wie groß ein aus Fragmenten zusammengesetztes PPP-Paket höchstens werden darf. Die MRRU entspricht somit auf der Seite des Peers der maximalen Größe eines PPP-Pakets, bevor es fragmentiert und über die einzelnen Verbindungen des Bündels verschickt wird.

Wird die MRRU nicht konfiguriert oder wird sie auf null gesetzt, wird die MRRU aus den MRUs der zum Bündel gehörenden Circuits automatisch berechnet.

Die MRRU ist als Vorschlag einer oberen Grenze zu sehen; der Peer kann eine kleinere MRRU aushandeln, falls er mit dem Vorschlag nicht einverstanden ist.

Standard-Einstellung: `CIRC_x_PPP_MRRU='0'`

Beispiel: `CIRC_1_PPP_MRRU='yes'`

Das nachfolgende Beispiel zeigt, wie man auf Client- und Server-Seite eine PPP-Multilink-Verbindung definiert. Dabei wird das Paket `pppoe` vorausgesetzt, welches die entsprechenden PPP-Module “ethernet” und “ethernet-server” mitbringt.

Beispiel (Client): Der Client “wotan” baut zwei zu einem Bündel zusammengefasste PPPoE-Verbindungen zum Server “odin” auf und authentifiziert sich mit Benutzernamen “user” und Passwort “pass”.

```

HOSTNAME='wotan'
OPT_BUNDLE='yes'
OPT_PPP='yes'
OPT_MULTILINK_PPP='yes'
OPT_PPP_ETHERNET='yes'
#
CIRC_N='3'
#
CIRC_1_NAME='ppp2odin'
CIRC_1_TYPE='ppp'
CIRC_1_ENABLED='yes'
CIRC_1_UP='yes'
CIRC_1_NETS_IPV4_N='1'
CIRC_1_NETS_IPV4_1='192.168.12.0/24'
CIRC_1_PPP_TYPE='bundle'
CIRC_1_PPP_USERID='user'
CIRC_1_PPP_PASSWORD='pass'
#
CIRC_2_NAME='ppp2odin-eth1'
CIRC_2_TYPE='ppp'
CIRC_2_ENABLED='yes'
CIRC_2_UP='yes'
CIRC_2_BUNDLE='ppp2odin'
CIRC_2_PPP_TYPE='ethernet'
CIRC_2_PPP_ETHERNET_DEV='eth1'
CIRC_2_PPP_ETHERNET_TYPE='kernel'
#
CIRC_3_NAME='ppp2odin-eth2'
CIRC_3_TYPE='ppp'
CIRC_3_ENABLED='yes'

```

```

CIRC_3_UP='yes'
CIRC_3_BUNDLE='ppp2odin'
CIRC_3_PPP_TYPE='ethernet'
CIRC_3_PPP_ETHERNET_DEV='eth2'
CIRC_3_PPP_ETHERNET_TYPE='kernel'

```

Beispiel (Server): Der Server “odin” wartet auf zwei Ethernet-Schnittstellen auf PPPoE-Verbindungsanfragen von Client “wotan” und verlangt eine Authentifizierung mit Benutzernamen “user” und Passwort “pass”. Diese PPPoE-Kanäle werden zu einem PPP-Bündel zusammengefasst. Weil keine Netze hin zum Client geroutet werden (CIRC\_1\_NETS\_IPV4\_N ist nicht definiert), muss via CIRC\_1\_PROTOCOLS='ipv4' explizit mitgeteilt werden, dass IPv4 über diese PPP-Verbindungen genutzt werden soll. Via CIRC\_1\_PPP\_LOCALIP und CIRC\_1\_PPP\_REMOTEIP wird konfiguriert, welche IPv4-Adressen der Client und der Server für diese PPP-Verbindung nutzen sollen.

```

HOSTNAME='odin'
OPT_BUNDLE='yes'
OPT_PPP='yes'
OPT_MULTILINK_PPP='yes'
OPT_PPP_ETHERNET_SERVER='yes'
OPT_PPP_PEERS='yes'
PPP_PEER_N='1'
PPP_PEER_1_USERID='user'
PPP_PEER_1_PASSWORD='pass'
PPP_PEER_1_CIRCUITS='ppp2wotan'
#
CIRC_N='3'
#
CIRC_1_NAME='ppp2wotan'
CIRC_1_TYPE='ppp'
CIRC_1_ENABLED='yes'
CIRC_1_UP='yes'
CIRC_1_PROTOCOLS='ipv4'
CIRC_1_PPP_TYPE='bundle'
CIRC_1_PPP_PEER_AUTH='yes'
CIRC_1_PPP_LOCALIP='192.168.222.1'
CIRC_1_PPP_REMOTEIP='192.168.222.2'
#
CIRC_2_NAME='ppp2wotan-eth1'
CIRC_2_TYPE='ppp'
CIRC_2_ENABLED='yes'
CIRC_2_UP='yes'
CIRC_2_BUNDLE='ppp2wotan'
CIRC_2_PPP_TYPE='ethernet-server'
CIRC_2_PPP_ETHERNET_DEV='eth1'
CIRC_2_PPP_ETHERNET_TYPE='kernel'
#
CIRC_3_NAME='ppp2wotan-eth2'
CIRC_3_TYPE='ppp'
CIRC_3_ENABLED='yes'
CIRC_3_UP='yes'
CIRC_3_BUNDLE='ppp2wotan'

```

```
CIRC_3_PPP_TYPE='ethernet-server'
CIRC_3_PPP_ETHERNET_DEV='eth2'
CIRC_3_PPP_ETHERNET_TYPE='kernel'
```

### 4.17.3. PPP-Circuits vom Typ “serial”

Dieser Circuit-Typ erlaubt es, PPP-Verbindungen zu einem anderen Rechner über eine serielle Leitung (ohne Modem) aufbauen zu können. Das Paket wird über die Variable `OPT_PPP_SERIAL` aktiviert:

**OPT\_PPP\_SERIAL** Diese Variable muss auf 'yes' gesetzt werden, um PPP-Circuits vom Typ “serial” anlegen zu können.

Standard-Einstellung: `OPT_PPP_SERIAL='no'`

Soll eine konkrete serielle Verbindung aufgebaut werden können, so muss ein passender Circuit konfiguriert werden, siehe Abschnitt [Circuit-Konfiguration](#) (Seite 86). Der zu verwendende Typ in `CIRC_x_TYPE` lautet “ppp”, der zu verwendende PPP-Typ in `CIRC_x_PPP_TYPE` lautet “serial”. Zu den allgemeinen Circuit-Variablen kommen die folgenden hinzu, die spezifisch für PPP/serial-Circuits sind:

**CIRC\_x\_PPP\_SERIAL\_DEV** Hier ist die serielle Schnittstelle anzugeben, die verwendet werden soll. Sie können entweder “com1” bis “com4” oder alternativ “ttyS0” bis “ttyS3” für die seriellen Schnittstellen 1–4 eintragen.

Beispiel: `CIRC_1_PPP_SERIAL_DEV='com2'`

**CIRC\_x\_PPP\_SERIAL\_SPEED** Hier muss die Übertragungsrate in Baud eingetragen werden. 38400 wird auch von alten Schnittstellen unterstützt. Eventuell kann es Probleme geben, wenn man die Rate auf 57600 oder gar 115200 Baud einstellt.

Beispiel: `CIRC_1_PPP_SERIAL_SPEED='38400'`

### 4.17.4. PPP-Circuits vom Typ “serial-server”

Dieser Circuit-Typ erlaubt es, PPP-Verbindungen von einem anderen Rechner über eine serielle Leitung (ohne Modem) annehmen zu können. Es entspricht in seiner Funktionsweise dem `OPT_PPP` in älteren fli4l-Versionen. Ein sinnvolles Anwendungsgebiet ist beispielsweise das Einbinden eines Notebook ohne Netzwerkkarte in das Netzwerk. Das Paket wird über die Variable `OPT_PPP_SERIAL_SERVER` aktiviert:

**OPT\_PPP\_SERIAL\_SERVER** Diese Variable muss auf 'yes' gesetzt werden, um PPP-Circuits vom Typ “serial-server” anlegen zu können.

Standard-Einstellung: `OPT_PPP_SERIAL_SERVER='no'`

Soll eine konkrete serielle Verbindung angenommen werden können, so muss ein passender Circuit konfiguriert werden, siehe Abschnitt [Circuit-Konfiguration](#) (Seite 86). Der zu verwendende Typ in `CIRC_x_TYPE` lautet “ppp”, der zu verwendende PPP-Typ in `CIRC_x_PPP_TYPE` lautet “serial-server”. Zu den allgemeinen Circuit-Variablen kommen die folgenden hinzu, die spezifisch für PPP/serial-server-Circuits sind:



**CIRC\_x\_PPP\_SERIAL\_SERVER\_DEV** Hier ist die serielle Schnittstelle anzugeben, die verwendet werden soll. Sie können entweder “com1” bis “com4” oder alternativ “ttyS0” bis “ttyS3” für die seriellen Schnittstellen 1–4 eintragen.

Beispiel: CIRC\_1\_PPP\_SERIAL\_SERVER\_DEV='com2'

**CIRC\_x\_PPP\_SERIAL\_SERVER\_SPEED** Hier muss die Übertragungsrate in Baud eingetragen werden. 38400 wird auch von alten Schnittstellen unterstützt. Eventuell kann es Probleme geben, wenn man die Rate auf 57600 oder gar 115200 Baud einstellt.

Beispiel: CIRC\_1\_PPP\_SERIAL\_SERVER\_SPEED='38400'

Beispiel (Client): Der Client “wotan” baut eine PPP-Verbindung zum Server “odin” auf und authentifiziert sich mit Benutzernamen “user” und Passwort “pass”.

```
HOSTNAME='wotan'
OPT_PPP='yes'
OPT_PPP_SERIAL='yes'
#
CIRC_N='1'
CIRC_1_NAME='ppp2odin'
CIRC_1_TYPE='ppp'
CIRC_1_ENABLED='yes'
CIRC_1_NETS_IPV4_N='1'
CIRC_1_NETS_IPV4_1='192.168.12.0/24'
CIRC_1_UP='yes'
CIRC_1_PPP_TYPE='serial'
CIRC_1_PPP_USERID='user'
CIRC_1_PPP_PASSWORD='pass'
CIRC_1_PPP_SERIAL_DEV='com1'
CIRC_1_PPP_SERIAL_SPEED='38400'
```

Beispiel (Server): Der Server “odin” wartet auf eine PPP-Verbindungsanfrage von Client “wotan” und verlangt eine Authentifizierung mit Benutzernamen “user” und Passwort “pass”. Weil keine Netze hin zum Client geroutet werden (CIRC\_1\_NETS\_IPV4\_N ist nicht definiert), muss via CIRC\_1\_PROTOCOLS='ipv4' explizit mitgeteilt werden, dass IPv4 über diese PPP-Verbindung genutzt werden soll. Via CIRC\_1\_PPP\_LOCALIP und CIRC\_1\_PPP\_REMOTEIP wird konfiguriert, welche IPv4-Adressen der Client und der Server für diese PPP-Verbindung nutzen sollen.

```
HOSTNAME='odin'
OPT_PPP='yes'
OPT_PPP_SERIAL_SERVER='yes'
OPT_PPP_PEERS='yes'
PPP_PEER_N='1'
PPP_PEER_1_USERID='user'
PPP_PEER_1_PASSWORD='pass'
PPP_PEER_1_CIRCUITS='ppp2wotan'
#
CIRC_N='1'
CIRC_1_NAME='ppp2wotan'
CIRC_1_TYPE='ppp'
CIRC_1_ENABLED='yes'
```

```

CIRC_1_PROTOCOLS='ipv4'
CIRC_1_UP='yes'
CIRC_1_PPP_PEER_AUTH='yes'
CIRC_1_PPP_LOCALIP='192.168.222.1'
CIRC_1_PPP_REMOTEIP='192.168.222.2'
CIRC_1_PPP_SERIAL_DEV='com1'
CIRC_1_PPP_SERIAL_SPEED='38400'

```

## 4.18. PPPOE - PPP über Ethernet

Dieses Paket erlaubt es, PPP-Verbindungen über ein Ethernet-Netzwerk aufzubauen. Dies wird in Deutschland vor allem für die Internet-Anbindung via DSL genutzt, wobei ein externes, über Ethernet angeschlossenes DSL-Modem genutzt wird. Zwischen dem fli4l-Router und dem DSL-Modem wird das Protokoll PPP benutzt, jedoch hier speziell über Ethernet (PPPoE<sup>21</sup>).

### 4.18.1. Ausgehende PPPoE-Verbindungen

Ein DSL-Zugang via PPPoE oder auch beliebige andere ausgehende PPPoE-Verbindungen werden generell als PPP-Circuit konfiguriert (siehe [Circuits vom Typ “ppp”](#) (Seite 225)), d. h. es gilt:

```
CIRC_x_TYPE='ppp'
```

Zusätzlich muss das OPT\_PPP\_ETHERNET aktiviert werden:

**OPT\_PPP\_ETHERNET** Diese Variable aktiviert die Unterstützung für ausgehende PPPoE-Verbindungen. Damit auch tatsächlich eine PPPoE-Verbindung genutzt werden kann, muss mindestens ein PPP-Circuit den Typ “ethernet” besitzen, d. h. es muss zusätzlich gelten

```

CIRC_x_TYPE='ppp'
CIRC_x_PPP_TYPE='ethernet'

```

(wobei “x” einen gültigen Circuit-Index darstellt).

Standard-Einstellung: OPT\_PPP\_ETHERNET='no'

Beispiel: OPT\_PPP\_ETHERNET='yes'

Zu den allgemeinen Circuit-Variablen kommen die folgenden, für PPP-Circuits des Typs “ethernet” spezifischen Variablen hinzu:

**CIRC\_x\_PPP\_ETHERNET\_DEV** Diese Variable enthält den Namen der Netzwerk-Schnittstelle, über die PPPoE genutzt werden soll. Dabei entspricht **eth0** der ersten Ethernet-Karte, **eth1** der zweiten Ethernet-Karte u. s. w.

Hat man nur eine Netzwerkkarte im Router, kann man das DSL-Modem ins LAN hängen, etwa indem man das DSL-Modem an den LAN-Switch mit anschließt. Dies ist jedoch nur die zweitbeste Lösung, weil die normalen IP-Pakete dann zusammen mit

<sup>21</sup>“Point-to-Point Protocol over Ethernet”, siehe RFC 2516

den PPPoE-Paketen im selben Netzsegment auftauchen und dies die maximale Übertragungsgeschwindigkeit negativ beeinflussen kann. Die beste Lösung ist die Nutzung einer separaten Netzwerkkarte für die Kommunikation mit dem DSL-Modem.

Beispiel: `CIRC_1_PPP_ETHERNET_DEV='eth1'`

**CIRC\_x\_PPP\_ETHERNET\_TYPE** PPPoE steht für die Übertragung von PPP-Paketen über Ethernet-Leitungen. Das bedeutet, dass die zu übertragenden Daten im ersten Schritt vom ppp-Dämon in PPP-Pakete und dann in einem zweiten Schritt für die Übertragung übers Ethernet nochmals in PPPoE-Pakete verpackt werden, um dann ans DSL-Modem geschickt zu werden. Das zweite Verpacken kann durch den pppoe-Dämon oder durch den Kern erfolgen. Mittels `CIRC_x_PPP_ETHERNET_TYPE` wird die Art und Weise der PPPoE-Paketerzeugung definiert, siehe hierzu Tabelle 4.21.

Wert	Beschreibung
kernel	Die PPP-Pakete werden direkt an den Linux-Kern gereicht, der daraus PPPoE-Pakete macht. Dadurch entfällt die Kommunikation mit einem zweiten Prozess und damit eine Menge Kopier- und Scheduling-Aufwand, was wiederum zu geringerer Prozessorlast führt. Dies ist die Standard-Methode, wenn nichts angegeben wurde.
daemon	Die Pakete werden durch den pppoe-Dämon erzeugt; die Kommunikation zwischen pppd und pppoe erfolgt asynchron. Das bedeutet, dass der Datenstrom mit Anfang- und Ende-Markern versehen wird, damit der pppoe-Dämon die einzelnen Pakete auseinanderhalten kann. Aufgrund des zweiten Prozesses und der zusätzlichen Markierungen ist diese Methode aufwändiger als die Methode "kernel" und sollte in der Regel nicht verwendet werden.

Tabelle 4.21.: Arten der PPPoE-Paketerzeugung

Standard-Einstellung: `CIRC_x_PPP_ETHERNET_TYPE='kernel'`

Beispiel: `CIRC_1_PPP_ETHERNET_TYPE='daemon'`

#### 4.18.2. Eingehende PPPoE-Verbindungen

Der fli4l kann auch konfiguriert werden, *eingehende* PPPoE-Verbindungen anzunehmen, also als ein Server zu fungieren. Solche PPPoE-Verbindungen werden ebenfalls als PPP-Circuit konfiguriert (siehe [Circuits vom Typ "ppp"](#) (Seite 225)), d. h. es gilt:

`CIRC_x_TYPE='ppp'`

Zusätzlich muss das `OPT_PPP_ETHERNET_SERVER` aktiviert werden:

**OPT\_PPP\_ETHERNET\_SERVER** Diese Variable aktiviert die Unterstützung für eingehende PPPoE-Verbindungen. Damit auch tatsächlich PPPoE-Verbindungen angenommen werden können, muss mindestens ein PPP-Circuit den Typ "ethernet-server" besitzen, d. h. es muss zusätzlich gelten

```
CIRC_x_TYPE='ppp'
CIRC_x_PPP_TYPE='ethernet-server'
```

(wobei “x” einen gültigen Circuit-Index darstellt).

Standard-Einstellung: OPT\_PPP\_ETHERNET\_SERVER='no'

Beispiel: OPT\_PPP\_ETHERNET\_SERVER='yes'

Zu den allgemeinen Circuit-Variablen kommen die folgenden, für PPP-Circuits des Typs “ethernet-server” spezifischen Variablen hinzu:

**CIRC\_x\_PPP\_ETHERNET\_SERVER\_DEV** Diese Variable enthält den Namen der Netzwerk-Schnittstelle, über die PPPoE genutzt werden soll. Dabei entspricht **eth0** der ersten Ethernet-Karte, **eth1** der zweiten Ethernet-Karte u. s. w.

Beispiel: CIRC\_1\_PPP\_ETHERNET\_SERVER\_DEV='eth1'

**CIRC\_x\_PPP\_ETHERNET\_SERVER\_TYPE** PPPoE steht für die Übertragung von PPP-Paketen über Ethernet-Leitungen. Das bedeutet, dass die zu übertragenden Daten im ersten Schritt vom ppp-Dämon in PPP-Pakete und dann in einem zweiten Schritt für die Übertragung übers Ethernet nochmals in PPPoE-Pakete verpackt werden. Das zweite Verpacken kann durch den pppoe-Dämon oder durch den Kern erfolgen. Mittels CIRC\_x\_PPP\_ETHERNET\_SERVER\_TYPE wird die Art und Weise der PPPoE-Paketerzeugung definiert, siehe hierzu Tabelle 4.21.

Standard-Einstellung: CIRC\_x\_PPP\_ETHERNET\_SERVER\_TYPE='kernel'

Beispiel: CIRC\_1\_PPP\_ETHERNET\_SERVER\_TYPE='daemon'

**CIRC\_x\_PPP\_ETHERNET\_SERVER\_SESSIONS** Diese Variable enthält die Anzahl der Verbindungen, die dieser PPPoE-Server maximal gleichzeitig verwalten kann.

Standard-Einstellung: CIRC\_x\_PPP\_ETHERNET\_SERVER\_SESSIONS='64'

Beispiel: CIRC\_1\_PPP\_ETHERNET\_SERVER\_SESSIONS='100'

### 4.18.3. Beispiele

Beispiel 1 (Internet-Zugang über PPPoE):

```
OPT_PPP='yes'                # PPP-Circuits aktivieren
OPT_PPP_ETHERNET='yes'      # PPPoE-Client-Circuits aktivieren
#
CIRC_N='1'
CIRC_1_NAME='DSL-Telekom'    # beliebig, aber eindeutig
CIRC_1_TYPE='ppp'           # das ist ein PPP-Circuit
CIRC_1_ENABLED='yes'
CIRC_1_NETS_IPV4_N='1'
CIRC_1_NETS_IPV4_1='0.0.0.0/0' # Default-Route ins Internet
CIRC_1_CLASS_N='1'
CIRC_1_CLASS_1='internet'   # Klasse für Internet-Anbindung
CIRC_1_UP='yes'             # beim Booten aktivieren
CIRC_1_TIMES='Mo-Su:00-24:0.0:Y'
CIRC_1_USEPEERDNS='yes'     # DNS-Server des Providers nutzen
```

## 4. Pakete

```
CIRC_1_PPP_TYPE='ethernet'      # PPPoE-Client
CIRC_1_PPP_USERID='anonymer'    # Benutzername zur Authentifizierung
CIRC_1_PPP_PASSWORD='surfer'    # Passwort zur Authentifizierung
CIRC_1_PPP_ETHERNET_TYPE='kernel' # Kernel soll PPPoE-Pakete packen
CIRC_1_PPP_ETHERNET_DEV='eth1'  # Karte, an der das DSL-Modem hängt
#
CIRC_CLASS_N='1'
CIRC_CLASS_1='internet'        # Klasse aller Internet-Circuits
```

Beispiel 2 (PPPoE-Server):

```
OPT_PPP='yes'                  # PPP-Circuits aktivieren
OPT_PPP_ETHERNET_SERVER='yes'  # PPPoE-Server-Circuits aktivieren
OPT_PPP_PEERS='yes'            # zum Speichern der Anmeldedaten
PPP_PEER_N='1'                 # 1x Anmeldedaten hinterlegen
PPP_PEER_1_USERID='user'       # Benutzername vom Client
PPP_PEER_1_PASSWORD='pass'     # Passwort vom Client
PPP_PEER_1_CIRCUITS='pppoe-eth1' # Anmeldedaten gelten für PPPoE-Circuit
#
CIRC_N='1'
CIRC_1_NAME='pppoe-eth1'       # beliebig, aber eindeutig
CIRC_1_TYPE='ppp'              # das ist ein PPP-Circuit
CIRC_1_ENABLED='yes'
CIRC_1_UP='yes'                # beim Booten aktivieren
CIRC_1_TIMES='Mo-Su:00-24:0.0:Y'
CIRC_1_PROTOCOLS='ipv4'        # IPv4 soll über die Verbindung laufen
CIRC_1_PPP_TYPE='ethernet-server' # PPPoE-Server
CIRC_1_PPP_PEER_AUTH='yes'     # Client-Authentifizierung ist Pflicht
CIRC_1_PPP_LOCALIP='192.168.222.1' # IP-Adresse des Servers
CIRC_1_PPP_REMOTEIP='192.168.222.2' # Start-IP-Adresse der Clients
CIRC_1_PPP_ETHERNET_SERVER_TYPE='kernel' # Kernel soll PPPoE-Pakete packen
CIRC_1_PPP_ETHERNET_SERVER_DEV='eth1'   # Ethernet-Karte für PPPoE
CIRC_1_PPP_ETHERNET_SERVER_SESSIONS='10' # max. 10 Clients
```

In der Dokumentation des PPP-Pakets im Abschnitt [“Multilink PPP”](#) (Seite 235) finden Sie ein Beispiel gebündelter PPPoE-Server-Verbindungen.

## 4.19. PROXY - Verschiedene Proxy-Server

## 4.20. QoS - Quality of Service

Mit QoS kann man die verfügbare Bandbreite regulieren und zum Beispiel auf verschiedene Ports, IP's und noch einiges mehr zu verteilen.

Ein Modem verwaltet eine Packet-Queue (Queue = Schlange, Reihe (in einer Schlange stehen)) in der Pakete gespeichert werden, die die verfügbare Bandbreite überschreiten. Bei DSL-Modems zum Beispiel, sind diese sehr groß. Das hat den Vorteil, dass recht gleichmäßig die maximale Bandbreite ausgenutzt werden kann. Denn schickt der Router an das Modem für kurze Zeit (sehr kurz) weniger Pakete, dann hat das Modem noch immer Pakete in der Queue, die es abzuarbeiten gilt. So eine Queue ist sehr simpel gehalten, denn dort geht alles der Reihe nach, ist eben ein faires Modem :-D

Und hier kommt dann QoS ins Spiel. QoS verwaltet auch eine Packet-Queue, nur eben im Router selber und dort hat man die Möglichkeit König zu sein, eben zu entscheiden welches Paket zu erst darf und welche Pakete sich noch ein bisschen zurückhalten müssen. Wenn alles richtig konfiguriert wurde, dann sendet QoS die Pakete gerade eben so schnell, dass sie nicht in die Packet-Queue des Modems landen. Das wäre so, als hätte man die Queue vom Modem in den Router geholt.

Noch etwas allgemeines zu den Geschwindigkeitseinheiten: QoS unterstützt Mibit/s (mebibit/s) und Kibit/s (kibibit/s), wobei gilt 1Mibit = 1024Kibit.

### 4.20.1. Konfiguration

**OPT\_QOS** Hier ist yes zusetzen wenn man das OPT\_QOS einsetzen will und no wenn man das Gegenteil beabsichtigt

**QOS\_INTERNET\_DEV\_N** Die Anzahl der Devices, die Daten ins Internet routen.

**QOS\_INTERNET\_DEV\_x** Hier sollte die Liste der Devices eingetragen werden, über die Daten ins Internet übertragen werden. Beispiele:

QOS_INTERNET_DEV_N='3'	Anzahl der Geräte
QOS_INTERNET_DEV_1='ethX'	für Kabel und sonstige Ethernet-Verbindungen
QOS_INTERNET_DEV_2='ppp0'	für DSL über PPPoE
QOS_INTERNET_DEV_3='ipppX'	für ISDN

Das ISDN-Device für den ersten Circuit dürfte das ippp0 lauten, für den 2. ippp1. Wenn aber für den ersten Circuit Kanalbündelung aktiviert wurde, dann heißt der 2. Kanal des 1. Circuit ippp1 und der 2. Circuit ippp2. Man sollte QOS mit ISDN nur dann nutzen, wenn Kanalbündelung für den benutzten Circuit deaktiviert ist.

**QOS\_INTERNET\_BAND\_DOWN** Maximale Downstreambandbreite des Internetzugangs. Siehe weiter oben: [Hinweis zu den Geschwindigkeitseinheiten](#) (Seite 246).

Hinweis: Für zeitkritische Aufgaben, wie das bevorzugen von ACK-Paketen, ist es nötig die Bandbreite nicht höher zu setzen als wirklich vorhanden, da man sonst zwar innerhalb der Packet-Queue auf dem Router die Pakete sortiert, dies dann aber nicht ganz korrekt gemacht wird und letztendlich doch wieder in der Packet-Queue des Modems aufgehalten werden. Möglich ist es außerdem, das die vom Provider angegebene Bandbreite nicht hundertprozentig mit der wirklich verfügbaren übereinstimmt, es könnte ein bisschen mehr oder auch weniger sein. Da ist also ausprobieren angesagt.

**QOS\_INTERNET\_BAND\_UP** Maximale Upstreambandbreite des Internet-Zugangs. Siehe Hinweis zu den Geschwindigkeitseinheiten unter OPT\_QOS.

Hinweis: Siehe Hinweis bei QOS\_INTERNET\_BAND\_DOWN.

**QOS\_INTERNET\_DEFAULT\_DOWN** Hier ist die Standardklasse für Pakete anzugeben, die aus dem Internet kommen. Alle Pakete, die nicht durch einen Filter in eine Klasse gesteckt wurden, landen dann in der angegebenen Klasse.

Wurde keine Klasse eingerichtet, für die die Variable

```
QOS_CLASS_x_DIRECTION='down'
```

gesetzt wurde, so setzt man:

```
QOS_INTERNET_DEFAULT_DOWN='0'
```

Beispiel:

Es wurden 2 Klassen eingerichtet und ein Filter steckt alle Pakete, die z.B. an eine bestimmte IP-Adresse geschickt wurden in die 1. von den beiden. Alle anderen Pakete sollen in die 2. Klasse gesteckt werden. Folglich müßte hier

```
QOS_INTERNET_DEFAULT_DOWN='2'
```

eingetragen werden.

Es ist darauf zu achten, dass für QOS\_INTERNET\_DEFAULT\_DOWN eine Klasse angegeben wird, deren QOS\_CLASS\_x\_DIRECTION Variable das Argument down enthält.

**QOS\_INTERNET\_DEFAULT\_UP** Hier ist die Standardklasse für Pakete anzugeben, die in das Internet gehen. Alle Pakete, die nicht durch einen Filter in eine Klasse gesteckt wurden, landen dann in der angegebenen Klasse.

Wurde keine Klasse eingerichtet, für die die Variable

```
QOS_CLASS_x_DIRECTION='up'
```

gesetzt wurde, so setzt man:

```
QOS_INTERNET_DEFAULT_UP='0'
```

Das ganze funktioniert analog zu QOS\_INTERNET\_DEFAULT\_DOWN.

Es ist darauf zu achten, dass für QOS\_INTERNET\_DEFAULT\_UP eine Klasse angegeben wird, deren QOS\_CLASS\_x\_DIRECTION Variable das Argument up enthält.

**QOS\_CLASS\_N** Hier ist die gewünschte Anzahl der Klassen (engl. Class) anzugeben.

**QOS\_CLASS\_x\_PARENT** Mit dieser Variable kann man Klassen verschachteln. Man gibt hier immer die Nummer der Vaterklasse an. Die Bandbreite die der Vaterklasse zugeteilt wurde, kann dann unter den Unterklassen weiter aufgeteilt werden. Die maximale Verschachtelungstiefe beträgt hier 8 Ebenen, wobei das Interface selber schon eine Ebene darstellt, es bleiben also maximal 7 konfigurierbar.

Soll die Klasse keine Unterklasse sein, so gibt man hier folgendes an:

```
QOS_CLASS_x_PARENT='0'
```

Ihr wird dann je nachdem zu welcher Richtung sie gehört (siehe QOS\_CLASS\_x\_PORT\_TYPE), maximal die in QOS\_CLASS\_x\_PORT\_TYPE oder QOS\_INTERNET\_BAND\_DOWN angegebene Bandbreite zugeteilt.

Wichtig: Falls hier nicht '0' angegeben wird, so ist darauf zu achten, dass die Vaterklasse vorher definiert wird (auf die Nummerierung bezogen).

**QOS\_CLASS\_x\_MINBANDWIDTH** Bandbreite, die man der Klasse zusprechen will. Man könnte hier auch von einem Verhältnis sprechen. Siehe Hinweis zu den Geschwindigkeitseinheiten unter `OPT_QOS`.

Beispiel: Man hat eine Klasse, dessen Bandbreite auf 128Kibit/s beschränkt ist.:

```
QOS_CLASS_1_MINBANDWIDTH='128Kibit/s'  
QOS_CLASS_1_MAXBANDWIDTH='128Kibit/s'  
QOS_CLASS_1_PARENT='0'
```

Weiterhin hat man 3 Klassen dessen `QOS_CLASS_x_MINBANDWIDTH`- und `QOS_CLASS_x_MAXBANDWIDTH`-Einstellungen wie folgt aussehen und alle Unterklassen unserer ersten Klasse sind:

```
QOS_CLASS_2_PARENT='1'  
QOS_CLASS_2_MINBANDWIDTH='60Kibit/s'  
QOS_CLASS_2_MAXBANDWIDTH='128Kibit/s'  
  
QOS_CLASS_3_PARENT='1'  
QOS_CLASS_3_MINBANDWIDTH='40Kibit/s'  
QOS_CLASS_3_MAXBANDWIDTH='128Kibit/s'  
  
QOS_CLASS_4_PARENT='1'  
QOS_CLASS_4_MINBANDWIDTH='28Kibit/s'  
QOS_CLASS_4_MAXBANDWIDTH='128Kibit/s'
```

Alle Unterklassen besitzen die selbe (oder auch keine) Priorität (siehe `QOS_CLASS_x_Prio`). Wird nun auf jede dieser 3 Klassen mehr Verkehr produziert als in ihrer jeweiligen `QOS_CLASS_x_MINBANDWIDTH` angegeben, so bekommt jede Klasse entsprechend ihrer `QOS_CLASS_x_MINBANDWIDTH`-Einstellung Bandbreite zugewiesen. Wenn aber z.B. Klasse 2 nur 20Kibit/s an Verkehr produziert, dann läßt dies Klasse ja 40Kibit/s "übrig". Dieser Überschuß wird im Verhältnis 40/28 unter Klasse 3 und 4 aufgeteilt. Jede Klasse selber ist durch `QOS_CLASS_x_MAXBANDWIDTH` auf 128Kibit/s beschränkt und da sie alle Unterklassen einer auf 128Kibit/s beschränkten Klasse sind, können sie auch alle zusammen nicht mehr als 128Kibit/s konsumieren.

**QOS\_CLASS\_x\_MAXBANDWIDTH** Bandbreite, die man der Klasse maximal zuteilen will. Es macht keinen Sinn einen niedrigeren Wert als der in `QOS_CLASS_x_MINBANDWIDTH` einzutragen. Gibt man hier nichts an, so nimmt diese Variable automatisch den Wert von `QOS_CLASS_x_MINBANDWIDTH` an. Eine solche Klasse kann dann natürlich keine überschüssige Bandbreite beanspruchen.

Siehe Hinweis zu den Geschwindigkeitseinheiten unter `OPT_QOS`.

**QOS\_CLASS\_x\_DIRECTION** Mit dieser Variable wird angegeben, zu welcher Richtung die Klasse gehört. Soll sie zur Regulierung des Upstreams benutzt werden, so ist hier

```
QOS_CLASS_x_DIRECTION='up'
```

anzugeben, für den Downstream analog:



#### 4. Pakete

```
QOS_CLASS_x_DIRECTION='down'
```

**QOS\_CLASS\_x\_PRIO** Hier wird geregelt, welche Priorität ein Klasse hat. Je niedriger die Nummer, desto höher die Priorität. Erlaubt sind werte zwischen 0 und 7. Wenn die Variable leer gelassen wird, so kommt das dem setzen einer 0 gleich.

Wenn eine Priorität gesetzt wird, dann wird darüber bestimmt, welcher Klasse zuerst Überschüssige Bandbreite angeboten wird. Um das klar zu machen, ändern wir das Beispiel aus QOS\_CLASS\_x\_MINIMUMBANDWIDTH leicht ab: An der ersten Klasse wird nichts verändert. Die Klassen 2-4 bekommen eine Priorität zugewiesen:

```
QOS_CLASS_2_PARENT='1'
QOS_CLASS_2_MINBANDWIDTH='60Kibit/s'
QOS_CLASS_2_MAXBANDWIDTH='128Kibit/s'
QOS_CLASS_2_PRIO='1'

QOS_CLASS_3_MINBANDWIDTH='40Kibit/s'
QOS_CLASS_3_PARENT='1'
QOS_CLASS_3_MAXBANDWIDTH='128Kibit/s'
QOS_CLASS_3_PRIO='1'

QOS_CLASS_4_PARENT='1'
QOS_CLASS_4_MINBANDWIDTH='28Kibit/s'
QOS_CLASS_4_MAXBANDWIDTH='128Kibit/s'
QOS_CLASS_4_PRIO='2'
```

Wie in dem Ursprungsbeispiel konsumiert Klasse 2 nur 20Kibit/s und läßt somit einen Überschuß von 40Kibit/s übrig. Klasse 3 und 4 wollen noch immer mehr Bandbreite als überhaupt verfügbar. Da nun aber Klasse 3 eine höhere Priorität als Klasse 4 hat, darf sie den Überschuß von 40Kibit/s vertilgen.

Angenommen Klasse 3 braucht aber nur 20Kibit/s des ursprünglichen Überschusses von 40Kibit/s, dann bekommt Klasse 4 die restlichen 20Kibit/s.

Nehmen wir nochmals etwas anderes an: Klasse 4 verbraucht gar keine Bandbreite und Klasse 2 und 3 wollen mehr als es überhaupt gibt. Dann bekommt jede erstmal ihre in QOS\_CLASS\_x\_MINBANDWIDTH angegebene Bandbreite und der Rest wird unter ihnen im 60/40 Verhältnis aufgeteilt, da beide Klassen die selbe Priorität haben.

Wie man also sieht beeinflußt QOS\_CLASS\_x\_PRIO nur, wie ein eventueller Bandbreitenüberschuß aufgeteilt wird.

**QOS\_CLASS\_x\_LABEL** Mit dieser optionalen Variable kann ein Label für die Klasse gesetzt werden. Dieses wird bei aktivem OPT\_RRDTOOL zur Beschriftung der Graphen von QOS genutzt.

**QOS\_FILTER\_N** Gewünschte Anzahl der der Filter angeben.

Zu den Filtern allgemein läßt sich noch folgendes sagen: Die Argumente von verschiedenen Variablen sind UND-verknüpft, mehrere Argumente der selben Variable sind ODER-verknüpft. Soll heißen: Wird zum Beispiel in einem und dem selben Filter nach einer

#### 4. Pakete

IP-Adresse und einem Port gefiltert, so werden nur Pakete herausgefiltert und in die Zielklasse(n) gesteckt, die auf beides gleichzeitig zutreffen.

Ein weiteres Beispiel: In einem und dem selben Filter sind zwei Ports (21 und 80) und eine IP-Adresse angegeben. Ein Datenpaket kann natürlich nicht von zwei Ports gleichzeitig kommen. Es verhält sich dann so: Der Filter filtert Pakete heraus, die entweder Port 21 benutzen und gleichzeitig die IP-Adresse, oder von Port 80 kommen und gleichzeitig von der IP-Adresse.

Wichtig: Es kommt auf die Reihenfolge der Filter an!

Ein Beispiel: Man möchte den Verkehr, der über den Port 456 läuft, für **alle** Rechner in Klasse A stopfen. Zusätzlich möchte man alle Pakete an den Rechner mit der IP 192.168.6.5 - bis auf die Pakete über Port 456 - in Klasse B laufen lassen. Richte ich nun den Filter mit der IP als erstes ein, dann landen alle Pakete - auch die über Port 456 laufen - in Klasse B und ein nachfolgender Filter für den Port 456 ändert auch nichts daran. Der Filter für den Port 456 muß also noch vor dem Filter mit der IP 192.168.6.5 stehen.

**QOS\_FILTER\_x\_CLASS** Mit dieser Variable stellt ihr ein, in welche Klasse das Paket, auf den dieser Filter zutrifft, gesteckt werden soll. Möchte man zum Beispiel die gefilterten Pakete in die Klasse, die mit den Variablen QOS\_CLASS\_25\_MINBANDWIDTH spezifiziert wurde, stecken, so müßte man hier

```
QOS_FILTER_x_CLASS='25'
```

setzen.

Mit QOS\_CLASS\_x\_DIRECTION gibt man ja an, ob eine Klasse nun zum Up- oder Downstream gehört. Wenn nun ein Filter gesetzt wird, der gefilterte Pakete zum Beispiel in eine Upstream-Klasse wandern läßt, dann werden auch nur Pakete aus dem Upstream von diesem Filter gefiltert und in die angegebene Klasse gesteckt. QOS\_CLASS\_x\_DIRECTION bestimmt also in welcher "Richtung" gefiltert wird.

Seit Version 2.1 ist es nun auch möglich mehr als eine Zielklasse anzugeben. Möchte man zum Beispiel den Verkehr über Port 456 sowohl für den Upstream als auch für den Downstream klassifizieren, so würde man hier

```
QOS_FILTER_x_CLASS='4 25'
```

angeben, wobei zum Beispiel Klasse Nummer 4 die Upstreamklasse ist und 25 die Downstreamklasse. Es macht keinen Sinn hier jeweils mehr als ein Up- und Downstreamklassen anzugeben, somit wird man auch nie mehr als zwei Zielklassen eintragen.

**QOS\_FILTER\_x\_IP\_INTERN** Hier können IP-Adressen und IP-Bereiche aus den internen Netzwerkwerken, nach denen gefiltert werden soll, angegeben werden. Sie sind durch Leerzeichen zu trennen und können frei kombiniert werden.

Das könnte zum Beispiel so aussehen:

```
QOS_FILTER_x_IP_INTERN='192.168.6.0/24 192.168.5.7 192.168.5.12'
```

#### 4. Pakete

Hier werden alle Adressen in der Form 192.168.6.X gefiltert und zusätzlich noch die IPs 192.168.5.7 und 192.168.5.12.

Diese Variable darf auch leer gelassen werden.

Wird diese Variable gleichzeitig mit `QOS_FILTER_x_IP_EXTERN` genutzt, so wird nur Verkehr gefiltert, der zwischen den in `QOS_FILTER_x_IP_INTERN` und `QOS_FILTER_x_IP_EXTERN` angegebenen IPs oder IP-Bereichen stattfindet.

**Wichtig:** Falls zusätzlich durch `QOS_FILTER_x_OPTION` nach `ACK`, `TOSMD`, `TOSMT`, `TOSMR` oder `TOSMC` gefiltert wird und die Variable `QOS_CLASS_x_DIRECTION` der Zielklasse 'down' entspricht, dann wird diese Variable ignoriert.

**QOS\_FILTER\_x\_IP\_EXTERN** Hier können IP-Adressen und IP-Bereiche aus dem externen Netzwerke (welches über `QOS_INTERNET_DEV` angebunden ist), nach denen gefiltert werden soll, angegeben werden. Sie sind durch Leerzeichen zu trennen und können frei kombiniert werden. Das ganze funktioniert analog zu `QOS_FILTER_x_IP_INTERN`.

Diese Variable darf auch leer gelassen werden.

**Wichtig:** Falls zusätzlich durch `QOS_FILTER_x_OPTION` nach `ACK`, `TOSMD`, `TOSMT`, `TOSMR` oder `TOSMC` gefiltert wird und die Variable `QOS_CLASS_x_DIRECTION` der Zielklasse 'down' entspricht, dann wird diese Variable ignoriert.

**QOS\_FILTER\_x\_PORT** Hier können Ports und Portranges angegeben werden, getrennt durch Leerzeichen und dürfen frei kombiniert werden. Falls die Variable leer ist, werden Übertragungen über sämtliche Ports limitiert.

Zu dem Format von Portranges: Möchte man nach Ports von 5000 bis 5099 filtern, so würde das folgender Maßen aussehen:

```
QOS_FILTER_x_PORT='5000-5099'
```

Ein weiteres Beispiel: Man möchte den Verkehr über die Ports 20 bis 21, 137 bis 139 und Port 80 filtern und in die selbe Klasse stecken lassen. Das sähe dann so aus:

```
QOS_FILTER_x_PORT='20-21 137-139 80'
```

Diese Variable darf auch leer gelassen werden.

Wichtig:

- Wenn nach Ports gefiltert wird, muß auch `QOS_FILTER_x_PORT_TYPE` entsprechend gesetzt werden.
- Wenn zusätzlich durch `QOS_FILTER_x_OPTION` nach `ACK`, `TOSMD`, `TOSMT`, `TOSMR` oder `TOSMC` gefiltert wird, dann werden Portranges ignoriert.

**QOS\_FILTER\_x\_PORT\_TYPE** Das Setzen dieser Variable ist nur wichtig im Zusammenhang mit `QOS_FILTER_x_PORT` und muß auch nur dann gesetzt werden (wird ansonsten ignoriert).

Da sich die Ports beim Clientbetrieb von den Ports beim Serverbetrieb unterscheiden, muss angegeben werden ob der Port des Servers oder Clients gemeint ist. Als Bezugspunkte gelten hier die Rechner aus dem eigenen Netz.

Folgende Einstellungen sind Möglich:

```
QOS_FILTER_x_PORT_TYPE='client'  
QOS_FILTER_x_PORT_TYPE='server'
```

Seit Version 2.1 ist auch die Kombination der beiden Argumenten möglich, um sowohl den Verkehr über den angegebenen Port aus dem eigenen Netz, als auch den Verkehr über selbigen Port aus dem Internet in die selbe Klasse zu stecken:

```
QOS_FILTER_x_PORT_TYPE='client server'
```

Dies entspricht der Erstellung von zwei ähnlichen Filtern, bei denen `QOS_FILTER_x_PORT_TYPE` einmal auf Client und einmal auf Server gesetzt wurde.

**QOS\_FILTER\_x\_OPTION** Mit dieser Variable kann man weitere Eigenschaften für den Filter aktivieren. Es darf hier höchstens eines der folgenden Argumente angegeben werden, denn eine Kombination dieser in ein und dem selben Filter macht keinen Sinn. Hingegen ist es sehr wohl möglich und auch teilweise sinnvoll, dass zum Beispiel ein Filter für ACK-Pakete und ein 2. Filter für TOSMD-Pakete ihre Pakete in die selbe Zielklasse leiten (siehe `QOS_FILTER_x_CLASS`).

**ACK** Acknowledgement-Pakete.

Ein Paket das auf diese Option zutrifft, wird als Bestätigung für ein Datenpaket zurückgesendet. Wenn ihr z.B. einen großen Download am laufen habt, dann kommen bei euch viele Datenpakete an und für jedes muß eine Antwort gesendet werden, dass das Datenpaket angekommen ist. Lassen diese Bestätigungspakete auf sich warten, so so wartet der Datenversender ab, bis diese eingetroffen sind, bevor er neue Datenpakete sendet, was euch nicht so richtig schmeckt.

Das ganze ist insbesondere wichtig bei asymmetrischen Verbindungen (ungleiche Up/Downstream-Bandbreite), wie sie bei den meisten privaten DSL-Angeboten üblich sind. Wird der meist relativ kleine Upstream an seine Grenzen gefahren, so stapeln sich die Pakete vor dem Ausgang förmlich auf und irgendwo in diesem riesigen Haufen sitzen hier und da die kleinen Bestätigungspakete. Im Normalfall geht das dann hübsch der Reihe nach. Bis das Bestätigungspaket dann an der Reihe ist, kann es gut sein, dass es so lange gedauert hat, dass unser Datenversender eine kleine Pause einlegt und was wie gesagt nicht gut für den Downstream ist.

Wir müssen also dafür sorgen, dass die Bestätigungspakete auf die Überholspur kommen, so dass sie in windeseile an allen "normalen" Paketen vorbeihuschen, damit sie auch noch rechtzeitig beim Datenversender ankommen. Wie sich dies Option sinnvoll mit einer Klasse kombinieren läßt, wird bei den Anwendungsbeispielen erläutert.

**ICMP** Ping-Pakete (Protokoll ICMP)

Ping-Pakete werden dazu benutzt, die Zeit zu messen, die ein Paket von A nach B braucht. Wenn ihr also ordentlich angeben wollt, dann gebt den Ping-Paketen z.B. eine höhere Priorität. Das hat jetzt nichts mit dem Spielen im Internet selber zu tun, also nicht denken nur weil ihr den Ping-Pakete den Vorrang gibt, dass ihr super niedrige Pingzeiten im Spiel bekommt...

### **IGMP** IGMP-Pakete (Protokoll IGMP)

Wenn IP-TV benutzt wird, ist es sinnvoll, das IGMP Protokoll zu filtern und zu priorisieren.

### **TCP**SMALL Kleine TCP Pakete

Durch diesen Filter können ausgehende HTTP(s)-Requests gefiltert priorisiert werden. Eine Kombination mit einem Zielpport ist möglich und sinnvoll. Größe der TCP Pakete: max. 800 Byte.

### **TCP** TCP-Pakete (Protokoll TCP)

Es wird nur nach Paketen gefiltert, die das Protokoll TCP benutzen.

### **UDP** UDP-Pakete (Protokoll UDP)

Es wird nur nach Paketen gefiltert, die das Protokoll UDP benutzen.

### **TOS\*** Type of Service

TOS steht für "Type of Service". Eine Applikation kann für jedes Paket was es verschickt eines der 4 TOS-Bits setzen. Damit wird angegeben welche Behandlung für die Pakete vorgesehen sind. So kann z.B. SSH TOS-Minimum-Delay für das Versenden der ein und Ausgabe setzen und TOS-Maximum-Troughput für das Versenden von Dateien. Generell benutzen Linux/Unix Programme diese Bits öfter als Windowsprogramme. Außerdem kann man z.B. auch in der Firewall die TOS-Bits für bestimmte Pakete setzen. Letztendlich kommt es dann aber auf die Router auf der Strecke an, ob die TOS-Bits beachtet werden, oder nicht. Wirklich von Interesse für einen fli4l sind aber eigentlich nur die TOS-Bits Minimum-Delay und Maximum-Throughput.

**TOSMD - TOS Minimum-Delay** Wird für Dienste benutzt, bei denen es wichtig ist, dass Pakete möglichst ohne Zeitverzögerung weitergeleitet werden. Empfohlen wird dieses TOS-Bit für FTP (Kontrolldaten), Telnet und SSH.

**TOSMT - TOS Maximum-Troughput** Wird für Dienste benutzt, bei denen es wichtig ist, dass große Datenmengen mit hoher Geschwindigkeit weitergeleitet werden. Empfohlen wird dieses TOS-Bit für FTP-Data und WWW.

**TOSMR - TOS Maximum-Reliability** Wird benutzt, wenn es wichtig ist, dass man eine gewisse Sicherheit hat, dass die Daten an ihr Ziel gelangen, ohne dass ein erneutes senden nötig ist. Empfohlen wird dieses TOS-Bit für SNMP und DNS.

**TOSMC - TOS Minimum-Cost** Wird benutzt, wenn es wichtig ist die Kosten der Datenübertragung zu Minimieren. Empfohlen wird dieses TOS-Bit für NNTP und SMTP.

### **DSCP\*** Differentiated Services Code Point

Mit DSCP bezeichnet man die Markierung nach RFC 2474. Dieses Verfahren hat 1998 die TOS Markierung weitestgehend abgelöst.

Die Filter auf DSCP-Klassen können wie folgt konfiguriert werden:

```
QOS_FILTER_x_OPTION='DSCPef'  
QOS_FILTER_x_OPTION='DSCPcs3'
```

Bitte beachten, dass DSCP groß und die Klasse kleingeschrieben wird.

Es können folgende Klassen verwendet werden:

af11-af13, af21-af23, af31-af33, af41-af43, cs1-cs7, ef und be (Standard)

### 4.20.2. Anwendungsbeispiele

Wie konfiguriert man OPT\_QoS nun genau? Dies wird nun an einigen Beispielen gezeigt:

- Beispiel 1: Ein einfaches Beispiel mit dem Ziel die Bandbreite auf 3 Rechner zu verteilen.
- Beispiel 2: Ein Beispiel mit dem Ziel die Bandbreite auf 2 Rechner zu verteilen und die jeweiligen Bandbreiten pro Rechner wiederum noch ein zweites mal aufzuteilen auf einen Port und den restlichen Verkehr des jeweiligen Rechners.
- Beispiel 3: Ein Beispiel, welches die allgemeine Funktionsweise von QoS versucht nahezubringen.
- Beispiel 4: Beispielkonfiguration für das Bevorteilen von ACK-Paketen, damit der Downstream bei gleichzeitig starkem Upstream nicht einbricht.

#### Beispiel 1

Ein einfaches Beispiel mit dem Ziel die Bandbreite auf 3 Rechner zu verteilen.

Dazu erstellen wir 4 Klassen (siehe QOS\_CLASS\_N und folgende) mit den jeweiligen Geschwindigkeiten (siehe QOS\_CLASS\_x\_MINBANDWIDTH / QOS\_CLASS\_x\_MINBANDWIDTH) und hängen sie an die Klasse 0 (siehe QOS\_CLASS\_x\_PARENT) also direkt an das Interface für “up” bzw. “down” (siehe QOS\_CLASS\_x\_DIRECTION).

Die vierte Klasse ist nur für eventuelle Besucher und bekommt weniger Bandbreite zugeteilt. Mit QOS\_INTERNET\_DEFAULT\_DOWN='4' lassen wir in diesem Fall allen nicht gefilterten Verkehr in die vierte “Gast”-Klasse wandern. Da wir aber selten Gäste haben und die Bandbreite für die anderen 3 Klassen jeweils die selbe beträgt, bekommt jeder Rechner 1/3 der gesamten Bandbreite, effektiv also 256Kibit/s.

Mit dieser Konfiguration haben wir allerdings erst das Grundgerüst erstellt. Jetzt müssen wir noch sagen welcher Verkehr durch welche Klasse geregelt werden soll.

Dazu benutzen wir Filter, welche den Verkehr den einzelnen Klassen zuordnen. Wir erstellen also 3 Filter für die 3 Rechner (siehe QOS\_FILTER\_N und folgende) und ordnen jeden Filter einer Klasse zu (siehe QOS\_FILTER\_x\_CLASS). Jetzt können wir mit QOS\_FILTER\_x\_IP\_INTERN, QOS\_FILTER\_x\_IP\_INTERN, QOS\_FILTER\_x\_PORT, QOS\_FILTER\_x\_PORT und QOS\_FILTER\_x\_OPTION bestimmen was durch die jeweilige Klasse zu der der Filter gehört geregelt werden soll.

Nennen wir das Interface 0 und die 3 Klassen 1, 2 und 3 und die 3 Filter F1, F2 und F3 ergibt sich das in Abbildung 4.5 dargestellte Szenario.

Die Konfiguration sieht dann so aus:

Drei Rechner nach IP gefiltert die je 1/3 bekommen falls kein Gast anwesend ist:

```
OPT_QOS='yes'
QOS_INTERNET_DEV_N='1'
QOS_INTERNET_DEV_1='ppp0'
QOS_INTERNET_BAND_DOWN='768Kibit/s'
QOS_INTERNET_BAND_UP='128Kibit/s'
```

#### 4. Pakete

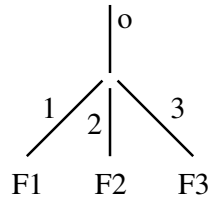


Abbildung 4.5.: Beispiel 1

```
QOS_INTERNET_DEFAULT_DOWN='4'  
QOS_INTERNET_DEFAULT_UP='0'
```

```
QOS_CLASS_N='4'
```

```
QOS_CLASS_1_PARENT='0'  
QOS_CLASS_1_MINBANDWIDTH='232Kibit/s'  
QOS_CLASS_1_MAXBANDWIDTH='768Kibit/s'  
QOS_CLASS_1_DIRECTION='down'  
QOS_CLASS_1_PRIO=''
```

```
QOS_CLASS_2_PARENT='0'  
QOS_CLASS_2_MINBANDWIDTH='232Kibit/s'  
QOS_CLASS_2_MAXBANDWIDTH='768Kibit/s'  
QOS_CLASS_2_DIRECTION='down'  
QOS_CLASS_2_PRIO=''
```

```
QOS_CLASS_3_PARENT='0'  
QOS_CLASS_3_MINBANDWIDTH='232Kibit/s'  
QOS_CLASS_3_MAXBANDWIDTH='768Kibit/s'  
QOS_CLASS_3_DIRECTION='down'  
QOS_CLASS_3_PRIO=''
```

```
QOS_CLASS_4_PARENT='0'  
QOS_CLASS_4_MINBANDWIDTH='72Kibit/s'  
QOS_CLASS_4_MAXBANDWIDTH='768Kibit/s'  
QOS_CLASS_4_DIRECTION='down'  
QOS_CLASS_4_PRIO=''
```

```
QOS_FILTER_N='3'
```

```
QOS_FILTER_1_CLASS='1'  
QOS_FILTER_1_IP_INTERN='192.168.0.2'  
QOS_FILTER_1_IP_EXTERN=''  
QOS_FILTER_1_PORT=''  
QOS_FILTER_1_PORT_TYPE=''  
QOS_FILTER_1_OPTION=''
```

```
QOS_FILTER_2_CLASS='2'  
QOS_FILTER_2_IP_INTERN='192.168.0.3'  
QOS_FILTER_2_IP_EXTERN=''
```

#### 4. Pakete

```
QOS_FILTER_2_PORT=''
QOS_FILTER_2_PORT_TYPE=''
QOS_FILTER_2_OPTION=''

QOS_FILTER_3_CLASS='3'
QOS_FILTER_3_IP_INTERN='192.168.0.4'
QOS_FILTER_3_IP_EXTERN=''
QOS_FILTER_3_PORT=''
QOS_FILTER_3_PORT_TYPE=''
QOS_FILTER_3_OPTION=''
```

Die Option `QOS_INTERNET_DEFAULT_UP` wurde auf 0 gesetzt da der Upstream nicht beschränkt werden soll.

### Beispiel 2

Ein Beispiel mit dem Ziel die Bandbreite auf 2 Rechner zu verteilen und die jeweiligen Bandbreiten pro Rechner wiederum noch ein zweites mal aufzuteilen auf einen Port und den restlichen Verkehr des jeweiligen Rechners.

Dazu erstellen wir erst einmal wieder 2 Klassen mit den jeweiligen Gesamtgeschwindigkeit und hängen sie direkt an das Interface für “up” bzw. “down” (siehe erstes Beispiel). Jetzt erstellen wir für den ersten Rechner an der ersten Klasse zwei weitere Klassen. Die Klassen werden genau so erstellt wie die beiden ersten Klassen direkt am Interface, allerdings mit einer Besonderheit: `QOS_CLASS_x_PARENT` ist jetzt nicht 0, sondern die Nummer der Klasse an die die Klassen angehängt werden sollen. Ist dies z. B. `QOS_CLASS_1`, so muss man jetzt `QOS_CLASS_1` von der Klasse die angehängt werden soll auf 1 setzen. Das gleiche wird für den zweiten Rechner auch gemacht. Man hängt wieder zwei Klassen an die Klasse für den zweiten Rechner. Dies kann man nun nicht nur für zwei Rechner machen, sondern für so viele wie man möchte. Auch kann man so viele Unterklassen an einer Klasse erstellen wie man möchte.

Hiermit haben wir wieder das Grundgerüst erstellt und müssen nun mit den Filtern den Verkehr den einzelnen Klassen zuordnen. (siehe erstes Beispiel)

Wir erstellen also 2 Filter für den ersten Rechner und 2 Filter für den zweiten Rechner. Jeweils einen Filter für den Port und einen Filter für den restlichen Verkehr vom Rechner. Hierbei ist unbedingt auf die Reihenfolge zu achten. Als erstes jeweils nur den Port und danach den Rest. Anders herum würde ja schon der Filter für den Rest alles einer Klasse zuordnen.

Nennen wir das Interface 0 und die 6 Klassen 1, 2, 3, 4, 5 und 6 und die 4 Filter F1, F2, F3 und F4 ergibt sich das in Abbildung 4.5 dargestellte Szenario.

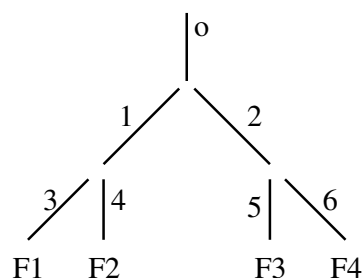


Abbildung 4.6.: Beispiel 2



#### 4. Pakete

Die Konfiguration sieht dann so aus:

Zwei Klassen für 2 Rechner die je 1/2 bekommen, und zwar vom Interface, mit jeweils 2 Klassen für einen Port der 2/3 bekommt und den Rest der 1/3 bekommt, und zwar jeweils von der Vaterklasse:

```
OPT_QOS='yes'
QOS_INTERNET_DEV_N='1'
QOS_INTERNET_DEV_1='ppp0'
QOS_INTERNET_BAND_DOWN='768Kibit/s'
QOS_INTERNET_BAND_UP='128Kibit/s'
QOS_INTERNET_DEFAULT_DOWN='7'
QOS_INTERNET_DEFAULT_UP='0'

QOS_CLASS_N='6'

QOS_CLASS_1_PARENT='0'
QOS_CLASS_1_MINBANDWIDTH='384Kibit/s'
QOS_CLASS_1_MAXBANDWIDTH='768Kibit/s'
QOS_CLASS_1_DIRECTION='down'
QOS_CLASS_1_PRIO=''

QOS_CLASS_2_PARENT='0'
QOS_CLASS_2_MINBANDWIDTH='384Kibit/s'
QOS_CLASS_2_MAXBANDWIDTH='768Kibit/s'
QOS_CLASS_2_DIRECTION='down'
QOS_CLASS_2_PRIO=''

QOS_CLASS_3_PARENT='1'
QOS_CLASS_3_MINBANDWIDTH='256Kibit/s'
QOS_CLASS_3_MAXBANDWIDTH='768Kibit/s'
QOS_CLASS_3_DIRECTION='down'
QOS_CLASS_3_PRIO=''

QOS_CLASS_4_PARENT='1'
QOS_CLASS_4_MINBANDWIDTH='128Kibit/s'
QOS_CLASS_4_MAXBANDWIDTH='768Kibit/s'
QOS_CLASS_4_DIRECTION='down'
QOS_CLASS_4_PRIO=''

QOS_CLASS_5_PARENT='2'
QOS_CLASS_5_MINBANDWIDTH='256Kibit/s'
QOS_CLASS_5_MAXBANDWIDTH='768Kibit/s'
QOS_CLASS_5_DIRECTION='down'
QOS_CLASS_5_PRIO=''

QOS_CLASS_6_PARENT='2'
QOS_CLASS_6_MINBANDWIDTH='128Kibit/s'
QOS_CLASS_6_MAXBANDWIDTH='768Kibit/s'
QOS_CLASS_6_DIRECTION='down'
QOS_CLASS_6_PRIO=''

QOS_FILTER_N='4'
```

```

QOS_FILTER_1_CLASS='3'
QOS_FILTER_1_IP_INTERN='192.168.0.2'
QOS_FILTER_1_IP_EXTERN=''
QOS_FILTER_1_PORT='80'
QOS_FILTER_1_PORT_TYPE='client'
QOS_FILTER_1_OPTION=''

QOS_FILTER_2_CLASS='4'
QOS_FILTER_2_IP_INTERN='192.168.0.2'
QOS_FILTER_2_IP_EXTERN=''
QOS_FILTER_2_PORT=''
QOS_FILTER_2_PORT_TYPE=''
QOS_FILTER_2_OPTION=''

QOS_FILTER_3_CLASS='5'
QOS_FILTER_3_IP_INTERN='192.168.0.3'
QOS_FILTER_3_IP_EXTERN=''
QOS_FILTER_3_PORT='80'
QOS_FILTER_3_PORT_TYPE='client'
QOS_FILTER_3_OPTION=''

QOS_FILTER_4_CLASS='6'
QOS_FILTER_4_IP_INTERN='192.168.0.3'
QOS_FILTER_4_IP_EXTERN=''
QOS_FILTER_4_PORT=''
QOS_FILTER_4_PORT_TYPE=''
QOS_FILTER_4_OPTION=''

```

Bei diesem Beispiel wurde die Option `QOS_INTERNET_DEFAULT_DOWN` so gewählt, dass der Verkehr, welcher nicht durch einen Filter einer Klasse zugeordnet wird, in eine nicht existierende Klasse gesteckt wird. Einfach aus dem Grund um das Beispiel zu vereinfachen und weil in dem Beispiel davon ausgegangen wird dass es keinen Rest gibt. Verkehr der in eine nicht existierende Klasse geleitet wird, wird nur sehr langsam weiter geleitet. Wenn es einen Rest gibt, ist also unbedingt darauf zu achten, dass dieser in eine eigene Klasse gesteckt wird, die auch existiert.

Die Option `QOS_INTERNET_DEFAULT_UP` wurde auf 0 gesetzt da der Upstream nicht beschränkt werden soll.

### Beispiel 3

Ein Beispiel, welches die allgemeine Funktionsweise von QoS versucht nahezubringen.

In Abbildung 4.7 ist noch einmal die Aufteilung aus dem zweiten Beispiel zu sehen, allerdings mit einer Erweiterung. An die Beiden Unterklassen der zweiten Klasse sind jeweils noch zwei weitere Unterklassen Angehängt. Es ist also möglich noch tiefer zu verschachteln. Es ist möglich, tiefer zu verschachteln als auf diesem Bild, die momentane Grenze liegt hier bei 8 Stufen, also man darf maximal nur 7 Weitere Stufen nach dem Interface erstellen, danach ist schluss. In die "Breite" ist allerdings keine Grenze gesetzt. Man kann also an eine Unterklasse innerhalb einer Stufe so viele Klassen anhängen wie man möchte.

Auf diesem Bild ist ausserdem noch zu erkennen, dass es auch möglich ist mehr als einen Filter an eine Klasse zu hängen, so wie es an der Klasse 10 geschehen ist. Aber auch bei

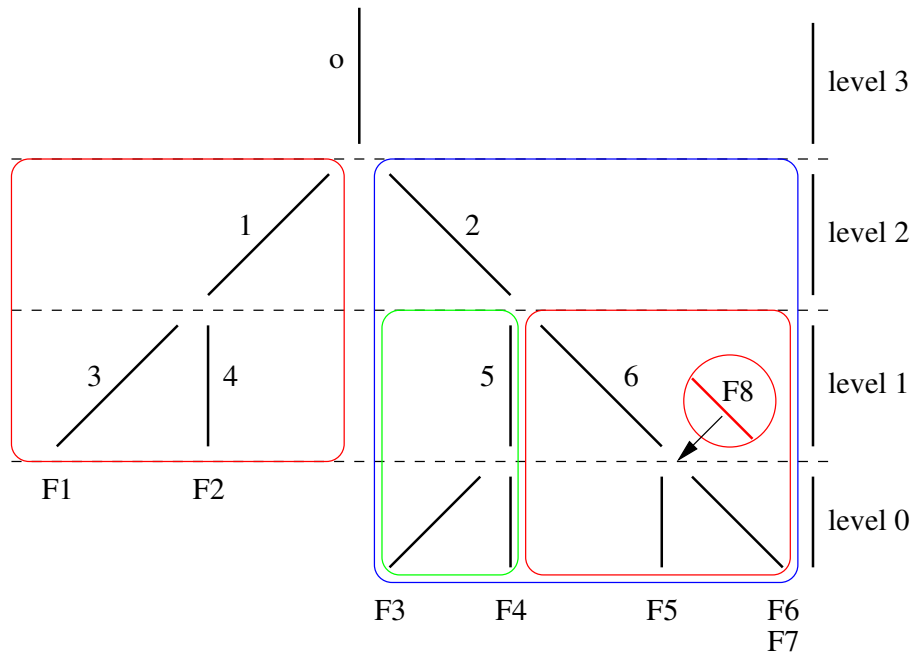


Abbildung 4.7.: Beispiel 3

den Filtern bleibt zu beachten dass es Momentan nicht möglich ist einen Filter mitten in den “Baum” zu heangen, so wie es mit F8 geschehen sollte.

Schauen wir uns nun als letztes noch den Sinn von Klassen und Unterklassen an. Klassen dienen dazu die Geschwindigkeit einer Verbindung einzustellen und zu regeln. Die Verteilung der Geschwindigkeit erfolgt wie bei QOS\_CLASS\_x\_MINBANDWIDTH beschrieben. Allerdings kann dies einen Nachteil haben wenn man z.b. alle Klassen an eine Klasse hängt. Möchte man z.b. einem Rechner die hälfte der bandbreite geben und dem zweiten ebenfalls die hälfte allerdings aufgeteilt auf 2/3 http und 1/3 Rest also jeweils 2/6 und 1/6 vom ganzen. So geschieht nun folgendes: bei Vollast bekommt jeder seine hälfte. Ueberträgt der zweite jedoch nichts über http so bleibt ja 2/6 über. Diese 2/6 bekommt jedoch nun nicht der 2. Rechner alleine, sondern es wird nach dem beschriebenen Verfahren aufgeteilt. Um dieses zu verhindern erstellt man Unterklassen. Der Verkehr einer Klasse wird somit erst an die Unklassen verteilt, erst wenn diese nicht den Kompletten Verkehr beanspruchen wird der Rest an andere Klassen Verteilt. In dem Bild sind jeweils die Bereiche eingekreist welche zusammengehoren. Rot = 1, Blau = 2, Grün = 5 und Orange = 6.

#### Beispiel 4

Beispielkonfiguration für das Priorisieren von ACK-Paketen, damit der Downstream bei gleichzeitig starkem Upstream nicht einbricht:

```
OPT_QOS='yes'
QOS_INTERNET_DEV_N='1'
QOS_INTERNET_DEV_1='ppp0'
QOS_INTERNET_BAND_DOWN='768Kibit/s'
QOS_INTERNET_BAND_UP='128Kibit/s'
```

#### 4. Pakete

```
QOS_INTERNET_DEFAULT_DOWN='0'  
QOS_INTERNET_DEFAULT_UP='2'
```

Hier konfigurieren wir ppp0 als Internetdevice (DSL) und geben die für TDSL (und einiger anderer Provider) übliche Up/Downstreambandbreiten an. Eventuell ist es nötig, dass wir die Upstreambandbreite noch um das eine oder andere Kibibit herabsetzen, das muß man ausprobieren.

Da wir keine Klassen für den Downstream einrichten wollen, setzen wir

```
QOS_INTERNET_DEFAULT_DOWN='0'
```

Für den Upstream soll die Klasse mit der Nummer 2 die Standardklasse sein. Das Netzwerkdevice ist eth0 und auf 10Mibit/s eingestellt.

```
QOS_CLASS_N='2'
```

```
QOS_CLASS_1_PARENT='0'  
QOS_CLASS_1_MINBANDWIDTH='127Kibit/s'  
QOS_CLASS_1_MAXBANDWIDTH='128Kibit/s'  
QOS_CLASS_1_DIRECTION='up'  
QOS_CLASS_1_PRIO=''
```

Dies ist die Klasse in die wir unsere ACK-(Bestätigungs-)Pakete hineinstecken wollen. Die ACK-Pakete sind recht klein und benötigen deswegen nur recht wenig Bandbreite. Trotzdem wollen wir sie eigentlich in keinsten Weise einschränken und teilen ihr 127Kibit/s zu. 1Kibit/s lassen wir übrig für den Rest.

```
QOS_CLASS_2_PARENT='0'  
QOS_CLASS_2_MINBANDWIDTH='1Kibit/s'  
QOS_CLASS_2_MAXBANDWIDTH='128Kibit/s'  
QOS_CLASS_2_DIRECTION='up'  
QOS_CLASS_2_PRIO=''
```

In diese Klasse soll dann der Rest (alles außer ACK-Pakete) hineingesteckt werden. Die Bandbreite, die wir dieser Klasse zuteilen sind die verbleibenden 1Kibit/s (128-127=1). Wir begrenzen sie aber auch nicht auf 1Kibit/s, begrenzt wird die Klasse durch den Eintrag

```
QOS_CLASS_2_MAXBANDWIDTH='128Kibit/s'
```

Da unsere erste Klasse die zugeteilte Bandbreite wohl kaum ausnutzen wird, bleibt also immer etwas übrig und das was übrig bleibt schnappt sich dann die zweite. Wenn man den Upstream noch weiter aufteilen möchte (was meist der Fall ist), so sind alle weiteren Klassen unter diese Klasse zu “hängen”. Dabei muß natürlich auch QOS\_INTERNET\_DEFAULT\_UP entsprechend angepaßt werden.

```
QOS_FILTER_N='1'
```

```
QOS_FILTER_1_CLASS='1'  
QOS_FILTER_1_IP_INTERN=''  
QOS_FILTER_1_IP_EXTERN=''  
QOS_FILTER_1_PORT=''  
QOS_FILTER_1_PORT_TYPE=''  
QOS_FILTER_1_OPTION='ACK'
```

Dieser Filter filtert alle Pakete, die auf die Option ACK zutreffen, also ACK-Pakete. Durch den Eintrag `QOS_FILTER_1_CLASS='1'` erreichen wir, dass diese gefilterten Pakete in die 1. Klasse gesteckt werden.

Zum Testen muß sucht man sich am besten eine gute oder mehrere Up- und Downloadquellen aus, von denen man weiß, dass sie sowohl den Up- als auch den Downstream voll auslasten können und läßt die Kabel glühen. Dabei sollte man einen Blick auf die Trafficanzeige des ImonC werfen. Am besten führt man das ganze auch mal ohne QoS durch.

Der Downstream sollte gar nicht oder wesentlich weniger stark einbrechen als ohne diese Konfiguration. Wie schon gesagt kann man die Lage noch verbessern, in dem man die Upstreambandbreite in Kibibit-Schritten herabsetzt und dann die Auswirkungen beobachtet. Bei mir wurde zum Beispiel das Optimum bei 121Kibit/s erreicht (kein Einbruch des Downstreams mehr). Dabei sind natürlich auch die MAXBANDWIDTH- und MINBANDWIDTH-Werte der Klassen entsprechend anzupassen.

### 4.21. SSHD - Secure Shell, Secure Copy

Eine Secure-Shell bietet die Möglichkeit, eine verschlüsselte Verbindung mit dem fli4l-Router aufzunehmen. Außerdem können mit dem Secure-Copy-Befehl Dateien verschlüsselt auf den fli4l-Router übertragen werden. Wird zusätzlich eine [Public Key Anmeldung](#) (Seite 264) benutzt, können Befehle auf dem fli4l-Router und Dateiübertragungen auch scriptgesteuert ausgeführt werden. Ab der Version 2.1.7 gibt es nur noch einen SSH2 Server.

#### 4.21.1. Installation des Secure-Shell-Dienstes

**OPT\_SSHD** Standard-Einstellung: `OPT_SSHD='no'`

Soll der Zugriff auf den Router mittels ssh ermöglicht werden, bedarf es der Änderung auf von `OPT_SSHD` auf `'yes'`. Dies installiert den ssh-Server Dropbear auf dem fli4l-Router. Dies ermöglicht auch das Kopieren von Dateien auf den Router.

**SSHD\_ALLOWPASSWORDLOGIN** Standard-Einstellung: `SSHD_ALLOWPASSWORDLOGIN='yes'`

Wird `SSHD_ALLOWPASSWORDLOGIN` auf `'no'` eingestellt, ist die Anmeldung mit ssh über ein Passwort auf dem fli4l-Router nicht mehr möglich. Die Anmeldung kann dann nur noch mittels privatem/öffentlichem Schlüsselpaar (private/public key) erfolgen. Dies setzt voraus, dass ein [öffentlicher Schlüssel](#) (Seite 264) auf dem Router hinterlegt ist.

**SSHD\_CREATEHOSTKEYS** Standard-Einstellung: `SSHD_CREATEHOSTKEYS='no'`

Ein ssh-Server benötigt einen sogenannten Hostkey, der weltweit einmalig sein sollte, damit sich der ssh-Server eindeutig gegenüber einem ssh-Client identifizieren kann. Das `sshd opt`-Paket liefert zwar einen Hostkey mit, um das erste Einloggen auf dem fli4l-Router per ssh-Client zu erlauben, aber der mitgelieferte Hostkey sollte so schnell wie möglich durch einen selbst generierten, nur Ihnen bekannten Hostkey ersetzt werden. Die Generierung eines eigenen Hostkeys ist deshalb so wichtig, weil nur auf diese Weise Schutz gegen so genannte Man-in-the-Middle-Attacks möglich ist. Ihr ssh-Client bemerkt es, wenn ein Cracker vorgibt, Ihr fli4l-Router zu sein, da dem Cracker dessen Hostkey nicht bekannt ist. Ihr ssh-Client warnt Sie daraufhin mit einer Meldung, dass der Hostkey sich geändert hat.

#### 4. Pakete

Die Erzeugung Ihres eigenen Hostkeys geschieht vollkommen automatisch, sobald Sie die Einstellung `SSHD_CREATEHOSTKEYS` auf 'yes' setzen. Dieser Vorgang ist sehr rechenintensiv und kann deshalb die Bootzeit um mehrere Minuten verlängern. Wenn der fli4l-Router mit aktiviertem `SSHD_CREATEHOSTKEYS` Eintrag startet, wird ein (oder mehrere) Hostkey(s) in dem Verzeichnis `/tmp/ssh` erzeugt. Die Dateien die dort stehen, kopieren Sie in das Verzeichnis `etc/ssh` unterhalb Ihres config Verzeichnisses (auf dem Rechner, auf dem sie fli4ls Bootmedium erzeugen). In meinem Fall sieht ein Directorylisting des config.babel Verzeichnisses so aus:

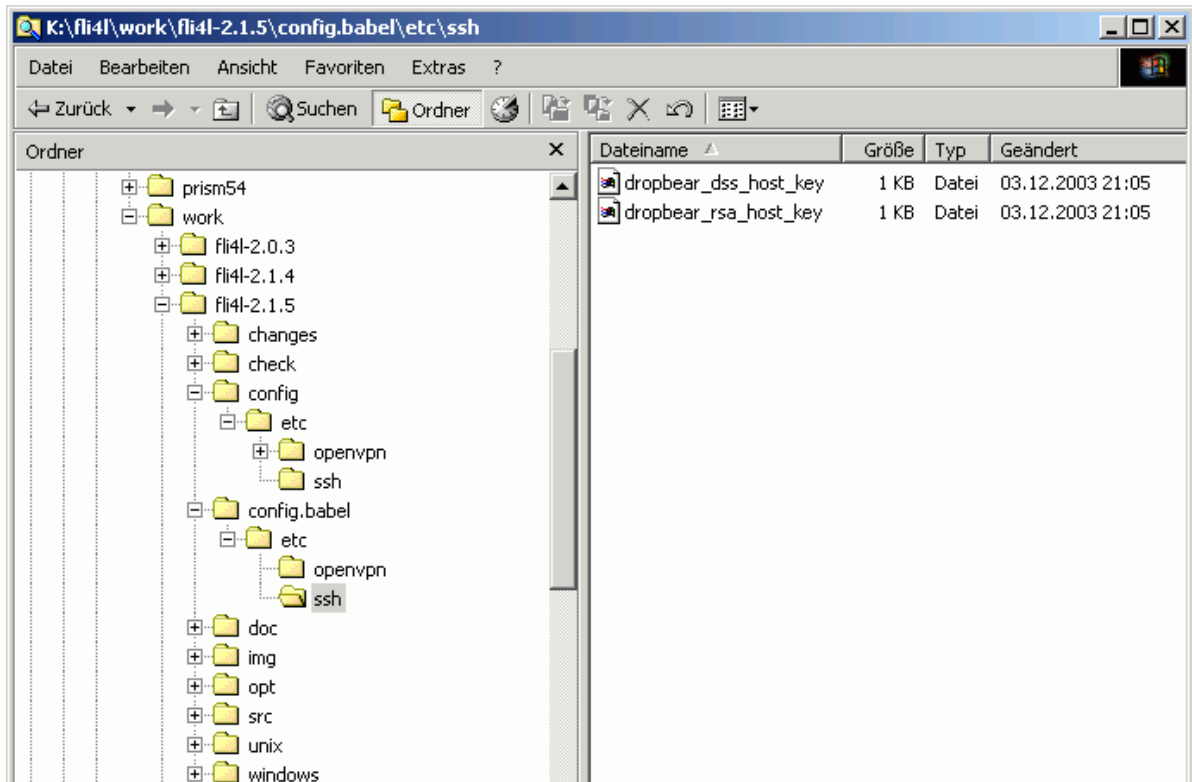


Abbildung 4.8.: Verzeichnisstruktur fli4l

Beachten Sie, dass unterhalb des `config` Verzeichnis erst das Verzeichnis `etc` kommt und darunter dann das Verzeichnis `ssh`. Und genau dorthin muss der oder die eben erzeugte(n) Hostkey(s) kopiert werden. Ab der fli4l Version 2.1.5 werden Dateien die unterhalb Ihres config Verzeichnisses stehen vorrangig vor den Dateien aus dem `opt` Verzeichnis behandelt. Dadurch werden bei dem nächsten Update Ihres fli4l-Routers die Dateien aus dem Verzeichnis `config/etc/ssh` eingebunden und nicht die Dateien, die im Verzeichnis `opt/etc/ssh` stehen. So ist es möglich für jeden fli4l-Router, den Sie konfigurieren, einen eigenen Hostkey zu benutzen. Wenn Sie die fli4l-Routerdateien erzeugen, erscheint ziemlich zum Schluss die Meldung „appending config specific files to opt.img ...“. Dort werden dann alle Dateien aufgelistet, die aus Ihrem config Verzeichnis kommen und nicht aus dem opt Verzeichnis.

#

```
# appending config specific files to opt.img ...
#
etc/ssh/dropbear_dss_host_key
etc/ssh/dropbear_rsa_host_key
```

Wenn Sie einen neuen Hostkey erzeugt haben, setzen Sie danach den Wert `SSHD_CREATEHOSTKEYS` wieder auf `'no'`, damit die Startskripte des fli4l-Routers nicht ständig einen neuen Hostkey generieren.

Wenn Sie sich nach dem Update des Hostkey auf Ihrem fli4l-Router anmelden, wird eine (je nach Programm unterschiedliche) Warnmeldung von Ihrem ssh-Client ausgegeben, die Sie auf einen geänderten Hostkey hinweist. Das ist normal, da Sie ja gerade den von fli4l mitgelieferten Hostkey gegen den von Ihnen erzeugten Hostkey ausgetauscht haben. Befolgen Sie die Hinweise Ihres ssh-Client, wie Sie den geänderten Hostkey permanent übernehmen können. Sollten Sie diese Warnmeldung zu einem späteren Zeitpunkt noch einmal bekommen, sollten Sie in jedem Fall prüfen, warum diese Warnung ausgegeben wurde und nicht einfach blind den geänderten Hostkey akzeptieren.

```

@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@   WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!   @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now (man-in-the-middle attack)!
It is also possible that the RSA host key has just been changed.
The fingerprint for the RSA key sent by the remote host is
ca:a4:ab:e7:af:d8:68:05:d3:1f:e6:15:08:d6:ed:36.
Please contact your system administrator.
Add correct host key in /home/babel/.ssh/known_hosts to get rid of this message.
Offending key in /home/babel/.ssh/known_hosts:7
Password authentication is disabled to avoid man-in-the-middle attacks.
```

#### **SSHD\_PORT** Standard-Einstellung: `SSHD_PORT='22'`

Mit `SSHD_PORT` kann abweichend vom Standard ein Port angegeben werden, auf dem der ssh-Server laufen soll.

Möchte man den ssh-Zugang auch von außen erlauben, ist [INPUT\\_ACCEPT\\_PORT\\_x](#) (Seite 49) anzupassen.

Die Befehle, um von einem Unix-/Linux-Rechner über das SSH-Protokoll auf fli4l zuzugreifen, lauten:

- `ssh` - Secure Shell
- `scp` - Secure Copy

Entsprechende Programme für Windows sind ebenso verfügbar, s. auch:

<http://www.chiark.greenend.org.uk/~sgtatham/putty/>

<http://winscp.net/eng/docs/lang:de>

<http://www.tectia.com/de/de.iw3>

**SSHD\_PUBLIC\_KEY\_N** Standard-Einstellung: `SSHD_PUBLIC_KEY_N='0'`

`SSHD_PUBLIC_KEY_N` beschreibt die Anzahl der öffentlichen Schlüssel, die auf den fli4l-Router kopiert werden sollen.

SSH gestattet die Authentifizierung mit Hilfe von asymmetrischen Verschlüsselungsverfahren. Dabei erfolgt die Authentifizierung anstatt über Nutzernamen und Passwort über Nutzernamen und einem Public-/Privatekey. Damit kann man sich die Eingabe eines Passwortes sparen. Das Schlüsselpaar erzeugt man mit Hilfe von `ssh-keygen` (oder `puttygen`, wenn `putty` unter Windows als ssh-Client eingesetzt wird). Optional kann beim Schlüsselerzeugen eine Passphrase (also ein Passwort, das man braucht, wenn man den Schlüssel benutzen will) vergeben werden, welche die Sicherheit noch zusätzlich erhöht. Benutzt man Passphrases sollte man über den Einsatz eines Schlüsselagenten nachdenken (siehe `ssh-agent` oder `pageant`).

**Wichtig:** *Der private Teil des Schlüsselpaares, ist so sorgfältig zu behandeln wie ein Passwort, da er die gleiche Funktion erfüllt. Der private Teil des Schlüssel wird bei dem ssh-Client hinterlegt. Der öffentliche Teil des Schlüssel wird für den fli4l-Router gebraucht und mit `SSHD_PUBLIC_KEY_x` oder `SSHD_PUBLIC_KEYFILE_x` zur Verfügung gestellt.*

Für weitere Informationen siehe die manual Pages von `ssh` und Konsorten bzw. die Dokumentation zu `putty` (<http://www.chiark.greenend.org.uk/~sgtatham/putty/>).

**SSHD\_PUBLIC\_KEY\_x** Für jeden Nutzer, der über `ssh` Zugang zum fli4l-Router erlangen möchte, kann hier der öffentliche Teil des Schlüssel angegeben werden. Am einfachsten geht das per Cut-and-Paste aus einem Terminalfenster heraus. Das könnte z.B. in etwa wie folgt aussehen:

```
SSHD_PUBLIC_KEY_1='1024 ... nutzernamen@hostname'
```

**Wichtig:** *Der Schlüssel enthält keine Zeilenumbrüche. Bei Cut-and-Paste aus `puttygen` heraus werden aber eventuell selbige eingefügt. Diese Zeilenumbrüche müssen wieder entfernt werden.*

Zur Zeit werden Schlüssel für die folgenden Verschlüsselungsverfahren unterstützt:

- DSA
- RSA
- ECDSA

**SSHD\_PUBLIC\_KEYFILE\_N** Standard-Einstellung: `SSHD_PUBLIC_KEYFILE_N='0'`

Anstatt den Inhalt des öffentlichen Teil des Schlüssel in die `sshd.txt` Datei zu kopieren, können Sie den öffentlichen Teil des Schlüssel auch direkt in das `opt`-Archiv kopieren lassen. Das funktioniert genauso wie bei `SSH_CREATEHOSTKEYS` beschrieben wurde. Kopieren Sie Ihren öffentlichen Teil des Schlüssel in das Verzeichnis `<config>/etc/ssh`.

**SSHD\_PUBLIC\_KEYFILE\_x** Der Dateiname des öffentlichen Teil des Schlüssel im `<config>/etc/ssh` Verzeichnis.

```
SSHD_PUBLIC_KEYFILE_1='root@fli4l'
```



Zur Zeit werden Schlüssel für die folgenden Verschlüsselungsverfahren unterstützt:

- DSA
- RSA
- ECDSA

**SSH\_CLIENT\_PRIVATE\_KEYFILE\_N** Standard-Einstellung:

```
SSH_CLIENT_PRIVATE_KEYFILE_N='0'
```

Wenn Sie mit dem ssh oder plink Client private Schlüssel zur Anmeldung an einen ssh Server benutzen wollen können Sie diese in das Verzeichnis `<config>/etc/ssh` kopieren. Das funktioniert genauso wie bei `SSH_CREATEHOSTKEYS` beschrieben wurde. Kopieren Sie Ihren privaten Teil des Schlüssel in das Verzeichnis `<config>/etc/ssh`. Private Schlüssel im OpenSSH-Format werden automatisch bei jedem Startvorgang von fli4l ins das dropbear-Format konvertiert.

**SSH\_CLIENT\_PRIVATE\_KEYFILE\_x** Der Dateiname des privaten Teil des Schlüssels im `<config>/etc/ssh` Verzeichnis.

```
SSHD_PRIVATE_KEYFILE_1='babel@rootserver'
```

Zur Zeit werden Schlüssel für die folgenden Verschlüsselungsverfahren unterstützt:

- DSA
- RSA
- ECDSA

### 4.21.2. Installation des dbclients

**OPT\_SSH\_CLIENT** Standard-Einstellung: `OPT_SSH_CLIENT='no'`

Wenn man einen reinen ssh2/scp Client benutzen möchte, kann man den dbclient von dropbear durch Setzen von `OPT_SSH_CLIENT='yes'` aktivieren. Dieser Client hat den Vorteil, dass er sich viel Programmcode mit dem dropbear ssh Server teilt. Dadurch wird sehr viel Platz im OPT-Archiv gespart. Der dbclient ist weitgehend kompatibel mit dem ssh/scp Client, die Befehlsparameter sind ähnlich. Es wird auch ein symbolischer Link auf `/usr/bin/ssh` bzw. `/usr/bin/scp` angelegt, damit ein gewohntes ssh `<host>` bzw. scp `<source> <target>` funktioniert.

Wenn man die dbclient bekannten Hostkeys permanent speichern will muss man die Datei `known_hosts` auf dem Verzeichnis `/.ssh` auf dem fli4l-Router in das `config/etc/ssh` kopieren. Das geschieht ähnlich wie mit einem erzeugten Hostkey. In dem folgenden Beispiel ist das ausgepackte fli4l Verzeichnis (in der die fli4l-Bootmedium erzeugt wird) in `/home/babel/fli4l-4.0.0-trunk-rpi-r60784` zu finden. Die Konfigurationsdateien liegen alle im Verzeichnis `config.babel`.

```
cd /home/babel/fli4l-4.0.0-trunk-rpi-r60784
mkdir -p config.babel/etc/ssh
scp fli4l:/.ssh/* config.babel/etc/ssh
```

### 4.21.3. Installation des plink Clients

**OPT\_PLINK\_CLIENT** Standard-Einstellung: `OPT_PLINK_CLIENT='no'`

Installiert auf dem fli4l-Router einen ssh1/ssh2/telnet Client. Das plink Programm ist die Unixversion des bekannten PuTTY Programms für Windows. Ein Aufruf von plink auf dem fli4l-Router gibt eine Hilfeseite für die Benutzung von plink aus.

Wenn man die plink bekannten Hostkeys permanent speichern will muss man die Datei `sshhostkeys` auf dem Verzeichnis `/.putty` auf dem fli4l-Router in das `config/etc/plink` kopieren. Das geschieht ähnlich wie mit einem erzeugten Hostkey. In dem folgenden Beispiel ist das ausgepackte fli4l Verzeichnis (in der das fli4l-Bootmedium erzeugt wird) in `/home/babel/fli4l-4.0.0-trunk-rpi-r60784` zu finden. Die Konfigurationsdateien liegen alle im Verzeichnis `config.babel`.

```
cd /home/babel/fli4l-4.0.0-trunk-rpi-r60784
mkdir -p config.babel/etc/plink
scp fli4l:/.putty/* config.babel/etc/plink
```

### 4.21.4. Installation des sftp-server

**OPT\_SFTPSERVER** Standard-Einstellung: `OPT_SFTPSERVER='no'`

Installiert auf dem fli4l-Router einen sftp-server.

### 4.21.5. Literatur

Dropbear SSH2 Site: <http://matt.ucc.asn.au/dropbear/dropbear.html>

Erste Version der Dokumentation von Claas Hilbrecht <babel@fli4l.de>, im April 2004

## 4.22. TOOLS - Zusätzliche Werkzeuge zum Debugging

Das Paket TOOLS liefert eine Reihe von Unix Programmen, die zumeist für Administrations- und Debugzwecke gedacht sind. Andere Programme wie `wget` werden z.B. dafür verwendet, die erste (Werbungs-)Seite einiger Provider abzufangen. Mit dem Wert `'yes'` wird das jeweilige Programm mit auf den fli4l-Router kopiert. Die Standardeinstellung ist `'no'`. Die Programme werden nur kurz vorgestellt, wie sie zu bedienen sind, entnehme man bitte den man Pages einer beliebigen Unix/ Linux Distribution oder online unter: <http://www.linuxmanpages.com>

### 4.22.1. Netzwerk-Tools

**OPT\_BMON** Bandbreitenmonitor

Das Programm `bmon` ist ein Monitor- und Debugging-Werkzeug um netzwerkbezogene Statistiken zu erheben und diese in einer nutzerfreundlichen Weise visuell aufbereitet anzuzeigen. Es werden verschiedene Ausgabemethoden unterstützt, unter anderem auch eine auf `curses` basierende interaktive Schnittstelle und eine programmierbare Ausgabe für Skripte.

**OPT\_CURL** Datenübertragungswerkzeug

## 4. Pakete

Das Programm curl erlaubt den Datentransfer von oder zu einem Server mit einer Reihe von unterstützten Protokollen. Dazu gehören u.a. FTP, HTTP(S), SCP, SFTP und TFTP.

Außerdem bietet das Programm Unterstützung für Benutzer-Authentifizierung, Datentransfer via Proxy, FTP-Upload, HTTP-POST-Anfragen, SSL-Verbindungen, Cookies, Wiederaufnahme abgebrochener Dateiübertragungen und mehr.

**Wichtig:** Um mit curl TLS-Verbindungen aufbauen zu können, sollten im Paket CERT via `CERT_X509_Mozilla='yes'` die Mozilla-X.509-Wurzelzertifikate installiert werden.

### OPT\_DIG Schweizer Taschenmesser fürs DNS

Der Befehl dig erlaubt es, vielfältige DNS-Abfragen durchzuführen.

### OPT\_FTP FTP-Client

Mit dem Programm ftp können eine FTP-Verbindung zu einem FTP-Server aufgebaut und Dateien zwischen Router und FTP-Server übertragen werden.

**FTP\_PF\_ENABLE\_ACTIVE** Die Einstellung `FTP_PF_ENABLE_ACTIVE='yes'` fügt dem Paketfilter eine Regel hinzu, die auf dem Router initiiertes aktives FTP ermöglicht. Bei `FTP_PF_ENABLE_ACTIVE='no'` muss eine solche Regel (falls gewünscht) manuell zum `PF_OUTPUT_%-Array` hinzugefügt werden, ein Beispiel ist in diesem [Abschnitt](#) (Seite 74) zu finden.

Passives FTP ist immer möglich, hierfür ist weder diese Variable noch eine explizite Paketfilter-Regel notwendig.

### OPT\_IFTOP Netzwerküberwachung

Mit dem Programm iftop wird eine Auflistung aller aktiven Netzwerkverbindungen und deren Durchsatz direkt auf dem fli4l angezeigt.

Das Programm iftop wird nach dem Anmelden auf dem fli4l-Router durch Eingabe von iftop gestartet.

### OPT\_IMONC Textorientiertes Steuerprogramm für imond

Dieses Programm liefert ein textorientiertes Frontend für den Router, um den imond zu steuern.

### OPT\_IPERF Performancemessung im Netzwerk

Mit dem Programm iperf kann eine Performancemessung des Netzwerks durchgeführt werden. Dazu wird das Programm auf den beiden beteiligten Testsystemen gestartet. Auf dem Server wird das Programm mit

```
fli4l-server 4.0.0-trunk-rpi-r60784~# iperf -s
```

```
-----  
Server listening on TCP port 5001  
TCP window size: 85.3 KByte (default)  
-----
```

gestartet. Der Server wartet dann auf eine Verbindung vom Client. Der Client wird durch

#### 4. Pakete

```
fli4l-client 4.0.0-trunk-rpi-r60784~# iperf -c 1.2.3.4
-----
Client connecting to 1.2.3.4, TCP port 5001
TCP window size: 16.0 KByte (default)
-----
[  3] local 1.2.3.5 port 50311 connected with 1.2.3.4 port 5001
[ ID] Interval      Transfer    Bandwidth
[  3]  0.0-10.0 sec   985 MBytes  826 Mbits/sec
```

gestartet. Sofort startet die Performancemessung und zeigt die ersten Ergebnisse an. iperf kennt noch eine Reihe weiterer Optionen, für Details schauen Sie sich bitte die Informationen auf der Homepage <http://iperf.sourceforge.net/> an.

#### **OPT\_LNSTAT** Erweiterte Netzwerk-Informationen

Dieses OPT installiert `lnstat`, ein Werkzeug zum Aufbereiten der Informationen in `/proc/net/stat`. Der Name steht für “Linux Network Statistics”.

Beispiele für `lnstat` aus dem Handbuch:

```
# lnstat -d
    Get a list of supported statistics files.
# lnstat -k arp_cache:entries,rt_cache:in_hit,arp_cache:destroys
    Select the specified files and keys.
# lnstat -i 10
    Use an interval of 10 seconds.
# lnstat -f ip_conntrack
    Use only the specified file for statistics.
# lnstat -s 0
    Do not print a header at all.
# lnstat -s 20
    Print a header at start and every 20 lines.
# lnstat -c -1 -i 1 -f rt_cache -k entries,in_hit,in_slow_tot
    Display statistics for keys entries, in_hit and in_slow_tot of field
    rt_cache every second.
```

#### **OPT\_NETCAT** Übertragen von Daten an TCP basierte Server

#### **OPT\_NETIO** Performancemessung im Netzwerk

Analog zu “iperf” kann mit “netio” eine Performancemessung des Netzwerks durchgeführt werden. Dazu wird das Programm auf den beiden beteiligten Testsystemen gestartet. Auf dem Server wird das Programm via `netio -s -t` (für Datenaustausch via TCP) bzw. `netio -s -u` (für Datenaustausch via UDP) gestartet. Auf dem Client wird dann via `netio <Server> -t` bzw. `netio <Server> -u` der zugehörige “netio”-Clientprozess gestartet, der dann das Programm auf dem Server kontaktiert und eine Messung vornimmt.

#### **OPT\_NGREP** Ein grep der direkt auf einem Netzwerkdevice arbeiten kann.

#### **OPT\_NMAP** Portscanner

Mithilfe von `nmap` können Betriebssysteme auf offene Ports untersucht werden. Weiterhin liefert das Programm auf Wunsch weitere Informationen z.B. zu MAC-Adressen oder dem verwendeten Betriebssystem.

**OPT\_NTTCP** Netzwerktest

Mit dem Programm NTTCP kann man die Netzwerkgeschwindigkeit testen. Dazu wird auf einer Seite ein Server gestartet und auf einer anderen Seite ein entsprechende Client.

Den Server startet man durch Eingabe von `nttcp -i -v`. Der Server wartet dann auf eine Testanforderung des Clients. Um jetzt z.B die Geschwindigkeit zu testen gibt man auf dem Client `nttcp -t <IP Adresse des Servers>` ein.

So sieht ein gestarteter nttcp Server aus:

```
fli4l-server 4.0.0-trunk-rpi-r60784~# nttcp -i -v
nttcp-l: nttcp, version 1.47
nttcp-l: running in inetd mode on port 5037 - ignoring options beside -v and -p
```

So sieht ein Test mit einem nttcp Client aus:

```
fli4l-client 4.0.0-trunk-rpi-r60784~# nttcp -t 192.168.77.77
1~~8388608~~~~4.77~~~~0.06~~~~14.0713~~~1118.4811~~~~2048~~~~429.42~~~34133.3
1~~8388608~~~~4.81~~~~0.28~~~~13.9417~~~239.6745~~~~6971~~~1448.21~~~24896.4
```

Die Hilfeseite von nttcp zeigt alle weiteren Parameter:

Usage: `nttcp [local options] host [remote options]`

local/remote options are:

```
-t      transmit data (default for local side)
-r      receive data
-l#     length of bufs written to network (default 4k)
-m      use IP/multicasting for transmit (enforces -t -u)
-n#     number of source bufs written to network (default 2048)
-u      use UDP instead of TCP
-g#us   gap in micro seconds between UDP packets (default 0s)
-d      set SO_DEBUG in sockopt
-D      don't buffer TCP writes (sets TCP_NODELAY socket option)
-w#     set the send buffer space to #kilobytes, which is
        dependent on the system - default is 16k
-T      print title line (default no)
-f      give own format of what and how to print
-c      compares each received buffer with expected value
-s      force stream pattern for UDP transmission
-S      give another initialisation for pattern generator
-p#     specify another service port
-i      behave as if started via inetd
-R#     calculate the getpid()/s rate from # getpid() calls
-v      more verbose output
-V      print version number and exit
-?      print this help
-N      remote number (internal use only)
default format is: %9b%8.2rt%8.2ct%12.4rbr%12.4cbr%8c%10.2rcr%10.1ccr
```

**OPT\_RTMON** Installiert ein tool, dass Änderungen der Routingtabelle überwacht. Primäre Verwendung: Debugging

**OPT\_SOCAT** Das Programm “socat” ist quasi eine verbesserte und mit mehr Funktionen “vollgestopfte” Version des “netcat”-Programms (Seite 268). Mit “socat” können nicht nur diverse Netzwerk-Verbindungen aufgebaut bzw. entgegengenommen werden, sondern auch Daten an UNIX-Sockets, Geräte, FIFOs etc. gesandt bzw. von dort ausgelesen werden. Insbesondere können Quellen und Ziele *verschiedener* Typen miteinander verbunden werden: Ein Beispiel wäre etwa ein via TCP auf einem Port horchender Netzwerk-Server, der empfangene Daten in einen lokalen FIFO schreibt bzw. Daten aus dem FIFO ausliest und diese dann übers Netzwerk an den Client schickt. Siehe <http://www.dest-unreach.org/socat/doc/socat.html> für mehr Informationen sowie Anwendungsbeispiele.

**OPT\_TCPDUMP** debug

Mit dem Programm tcpdump kann Netzwerkverkehr beobachtet, ausgewertet mitgeschnitten werden. Mehr dazu unter z.B. Google mit den Suchworten “tcpdump man”  
tcpdump <parameter>

**OPT\_TRACEPATH** Ermittlung der PMTU

Mit dem Programm `tracepath` kann die so genannte “Path MTU” ermittelt werden. Das ist die maximal verwendbare Paketgröße auf dem Pfad vom fli4l-Router zum Zielhost. Größere Pakete müssen entweder fragmentiert werden (IPv4) oder werden verworfen (IPv6). Typischerweise sorgt sich der Linux-Kernel um die Ermittlung der korrekten Path MTU (Stichwort “Path MTU Discovery”). Gelegentlich ist es jedoch nützlich, diese Path MTU herauszufinden, um Probleme im Netzwerk zu finden.

Ein Beispiel für IPv4:

```
sandbox 4.0.0-r46077M # tracepath -4 fli4l.de
1?: [LOCALHOST] pmtu 1500
1: fritz.box 0.703ms
1: fritz.box 0.588ms
2: a89-182-53-190.net-http.de 0.702ms pmtu 1492
2: a81-14-248-243.net-http.de 33.692ms
3: a81-14-249-82.net-http.de 32.089ms asymm 4
4: xe-4-1-2.edge4.Berlin1.Level3.net 35.936ms
5: SYSELEVEN-G.edge4.Berlin1.Level3.net 74.944ms asymm 8
6: ecix.dus.octalus.in-berlin.de 49.693ms asymm 7
7: virtualhost.in-berlin.de 50.269ms reached
Resume: pmtu 1492 hops 7 back 57
```

Hier erfolgt die Internet-Anbindung über eine DSL-Verbindung zwischen einer AVM Fritz!Box und einem BRAS des Internet-Providers http. Da für DSL in Deutschland PPP-over-Ethernet (PPPoE) verwendet wird, ist die Path MTU nur 1492 Byte groß.

Ein Beispiel für IPv6:

```
sandbox 4.0.0-r46077M # tracepath -6 fli4l.de
```

#### 4. Pakete

```
1?: [LOCALHOST] 0.046ms pmtu 1280
1: gw-1362.ham-01.de.sixxs.net 43.586ms
1: gw-1362.ham-01.de.sixxs.net 42.832ms
2: 2001:6f8:862:1::c2e9:c729 43.565ms asymm 1
3: 2001:6f8:862:1::c2e9:c72c 44.313ms asymm 2
4: 30gigabitethernet4-3.core1.fra1.he.net 64.501ms asymm 6
5: no reply
6: virtualhost.in-berlin.de 65.949ms reached
Resume: pmtu 1280 hops 6 back 56
```

Hier erfolgt die Internet-Anbindung über einen 6in4-Tunnel von SixXS. In der Konfiguration des Tunnels ist eine Tunnel-MTU von 1280 fest eingestellt. Da dies die kleinste erlaubte MTU für IPv6-Verbindungen ist, wird sie nirgendwo anders auf dem Pfad zum Zielhost weiter reduziert.

#### **OPT\_DHCPDUMP** DHCP packet dumper

Mit dem Programm `dhcpcdump` können DHCP Pakete genauer analysiert werden. Das Programm setzt auf `tcpdump` auf und erzeugt leicht lesbare Ausgaben.

Benutzung:

```
dhcpcdump -i interface [-h regular-expression]
```

Gestartet wird das Programm also bspw. mit folgendem Aufruf:

```
dhcpcdump -i eth0
```

Falls gewünscht, kann mit Hilfe regulärer Ausdrücke auch direkt auf eine bestimmte MAC-Adresse gefiltert werden. Der Aufruf sieht dann so aus:

```
dhcpcdump -i eth0 -h ^00:a1:c4
```

Die Ausgabe könnte dann z.B. so aussehen:

```
TIME: 15:45:02.084272
IP: 0.0.0.0.68 (0:c0:4f:82:ac:7f) > 255.255.255.255.67 (ff:ff:ff:ff:ff:ff)
OP: 1 (BOOTPREQUEST)
HTYPE: 1 (Ethernet)
HLEN: 6
HOPS: 0
XID: 28f61b03
SECS: 0
FLAGS: 0
CIADDR: 0.0.0.0
YIADDR: 0.0.0.0
SIADDR: 0.0.0.0
GIADDR: 0.0.0.0
CHADDR: 00:c0:4f:82:ac:7f:00:00:00:00:00:00:00:00:00:00
```

```

SNAME: .
FNAME: .
OPTION: 53 ( 1) DHCP message type          3 (DHCPREQUEST)
OPTION: 54 ( 4) Server identifier           130.139.64.101
OPTION: 50 ( 4) Request IP address          130.139.64.143
OPTION: 55 ( 7) Parameter Request List      1 (Subnet mask)
                                              3 (Routers)
                                              58 (T1)
                                              59 (T2)

```

### OPT\_WGET http/ftp Client

Mit dem Programm wget können Daten von einem Webserver im Batch abgerufen werden. Praktisch ist aber (und deswegen ist wget im fli4l-Paket dabei), dass man damit Umlenkungen des Providers auf den eigenen Webserver nach einem Verbindungsaufbau auf einfache Weise abfangen kann, z.B. für Freenet. Wie das geht, hat Steffen Peiser in einem Mini-HowTo erklärt.

Siehe: <http://www.fli4l.de/hilfe/howtos/einsteiger/wget-und-freenet/>

**Wichtig:** *Um mit wget TLS-Verbindungen aufbauen zu können, sollten im Paket CERT via CERT\_X509\_MOZILLA='yes' die Mozilla-X.509-Wurzelzertifikate installiert werden.*

### 4.22.2. Die Hardware-Erkennung

Oftmals weiß man nicht genau, welche Hardware im eigenen Rechner steckt bzw. welche Treiber man nun genau für seine Netzwerkkarte oder seinen USB-Chipsatz verwenden soll. Die Hardware kann an der Stelle helfen. Sie liefert eine Liste von Geräten im Rechner und wenn möglich den dazugehörigen Treiber. Man kann dabei auswählen, ob die Erkennung gleich beim Booten erfolgen soll (was sich vor einer Erstinstallation empfiehlt) oder später bei laufendem Rechner bequem über das Web-Interfaces getriggert werden soll. Die Ausgabe könnte dabei z.B. wie folgt aussehen:

```

fli4l 4.0.0-trunk-rpi-r60784 # cat /bootmsg.txt
#
# PCI Devices and drivers
#
Host bridge: Advanced Micro Devices [AMD] CS5536 [Geode companion] Host Bridge (rev 33)
Driver: 'unknown'
Entertainment encryption device: Advanced Micro Devices [AMD] Geode LX AES Security Block
Driver: 'geode_rng'
Ethernet controller: VIA Technologies, Inc. VT6105M [Rhine-III] (rev 96)
Driver: 'via_rhine'
Ethernet controller: VIA Technologies, Inc. VT6105M [Rhine-III] (rev 96)
Driver: 'via_rhine'
Ethernet controller: VIA Technologies, Inc. VT6105M [Rhine-III] (rev 96)
Driver: 'via_rhine'
Ethernet controller: Atheros Communications, Inc. AR5413 802.11abg NIC (rev 01)
Driver: 'unknown'
ISA bridge: Advanced Micro Devices [AMD] CS5536 [Geode companion] ISA (rev 03)
Driver: 'unknown'

```



```
IDE interface: Advanced Micro Devices [AMD] CS5536 [Geode companion] IDE (rev 01)
Driver: 'amd74xx'
USB Controller: Advanced Micro Devices [AMD] CS5536 [Geode companion] OHC (rev 02)
Driver: 'ohci_hcd'
USB Controller: Advanced Micro Devices [AMD] CS5536 [Geode companion] EHC (rev 02)
Driver: 'ehci_hcd'
```

Hier stecken also im wesentlichen 3 Netzwerkkarten drin, die vom 'via\_rhine'-Treiber verwaltet werden und eine Atheros-Wlan-Karte, die vom madwifi-Treiber verwaltet wird (der Name wird noch nicht korrekt aufgelöst).

**OPT\_HW\_DETECT** Diese Variable sorgt dafür, dass die für die Hardware-Erkennung Dateien auf dem Router landen. Man kann sich die Ergebnisse dann entweder nach dem Booten auf der Konsole ansehen, wenn man `HW_DETECT_AT_BOOTTIME` auf 'yes' gesetzt hat oder im Web-Interface ansehen, wenn man **OPT\_HTTPD** (Seite 165) auf 'yes' gesetzt hat. Im Web-Interface kann man sich natürlich auch den Inhalt von '/bootmsg.txt' ansehen, wenn man schon einen funktionierenden Netzzugang hat.

**HW\_DETECT\_AT\_BOOTTIME** Startet die Hardware-Erkennung beim Booten. Die Erkennung läuft im Hintergrund (sie dauert ein wenig) und schreibt dann ihre Ergebnisse auf die Konsole und nach '/bootmsg.txt'.

**OPT\_LSPCI** Auflisten aller PCI-Geräte

**OPT\_I2CTOOLS** Tools für I<sup>2</sup>C Zugriffe.

**OPT\_IWLEEPROM** Tool zum Zugriff auf das EEPROM von Intel und Atheros WLAN Karten.

Wird benötigt um z.B. bei ath9k Karten die Reg-Domain passend zu setzen (siehe <http://blog.asiantuntijakaveri.fi/2014/08/one-of-my-atheros-ar9280-minipcie-cards.html>).

**OPT\_ATH\_INFO** Tool zur Hardwarediagnose von WLAN Karten mit Atheros Chipsatz.

Mithilfe dieses Tools können z.B. bei ath5k WLAN Karten detaillierte Informationen über die verwendete Hardware gewonnen werden. Dazu gehören z.B. der verwendete Chipsatz oder Angaben zur Kalibrierung.

**OPT\_FLASHROM** Tool zum flashen von Chipsätzen.

Mithilfe dieses Tools können z.B. PC Engines Boards mit einem neuen BIOS oder einer neuen Firmware versorgt werden. Näheres dazu findet sich auf <http://www.flashrom.org>.

### 4.22.3. Dateien-Tools

**OPT\_E3** Ein Editor für fli4l

Dies ist ein sehr kleiner, in Assembler geschriebener Editor. Er stellt verschiedene Editor-Modi zur Verfügung, die andere („große“) Editoren nachstellen. Um einen bestimmten Modus zu wählen, reicht es e3 mit dem richtigen Befehl zu starten. Eine Kurzübersicht der Tastenbelegung bekommt man, wenn man e3 ohne Parameter startet oder Alt+H drückt

(außer im VI-Modus, dort muß man im CMD-Modus „:h“ eintippen). Zu beachten ist auch, dass das Caret-Zeichen (^) für die Ctrl-/Strg-Taste steht.

Befehl	Modus
e3 / e3ws	WordStar, JOE
e3vi	VI, VIM
e3em	Emacs
e3pi	Pico
e3ne	NEdit

**OPT\_MTOOLS** Die mtools stellen eine Reihe von DOS-ähnlichen Befehlen zum vereinfachten Umgang (Kopieren, Formatieren, etc.) mit DOS-Datenträgern bereit.

Die genaue Syntax der Befehle kann in der Dokumentation von mtools nachgeschlagen werden:

<http://www.gnu.org/software/mtools/manual/mtools.html>

**OPT\_SHRED** Installiert das Programm *shred* auf dem Router, ein Programm zum gründlichen Löschen von Blockgeräten.

**OPT\_YTREE** Datei-Manager

Installiert Datei-Manager Ytree auf dem Router.

#### 4.22.4. Entwickler-Tools

**OPT\_OPENSSL** Mit dem Programm openssl können z.B. Test der Cryptobeschleuniger durchgeführt werden.

```
openssl speed -evp des -elapsed
openssl speed -evp des3 -elapsed
openssl speed -evp aes128 -elapsed
```

**OPT\_STRACE** debug

Mit dem Programm strace können die Funktionsaufrufe, der Ablauf eines Programmes beobachtet werden

```
strace <programm>
```

**OPT\_REAVER** Brute force Angriff aus Wifi WPS PINs

Testet alle möglichen WPS PINS aus um das WPA Passwort zu ermitteln. Details für die Verwendung auf der Kommandozeile bitte nachlesen unter:

<http://code.google.com/p/reaver-wps/>

**OPT\_VALGRIND** Installiert Valgrind auf dem Router.

### 4.23. UMTS - Anbindung mittels UMTS an das Internet

Dieses Paket stellt die Funktion zur Verfügung, den fli4l-Router mittels UMTS an das Internet anzubinden. Für den Betrieb sind unter anderem auch weitere optionale Pakete erforderlich.

Ein UMTS-Zugang wird generell als spezieller PPP-Circuit konfiguriert (siehe [Circuits vom Typ "ppp"](#) (Seite 225)), d. h. es gilt:

```
CIRC_x_TYPE='ppp'  
CIRC_x_PPP_TYPE='umts'
```

Weitere, UMTS-spezifische (Circuit-)Einstellungen werden in den folgenden Abschnitten erläutert.

### 4.23.1. Allgemeine UMTS-Konfiguration

**OPT\_UMTS** Diese Variable aktiviert die Unterstützung für UMTS. Damit auch tatsächlich eine UMTS-Verbindung genutzt werden kann, muss mindestens ein PPP-Circuit den Typ “umts” besitzen, d. h. es muss zusätzlich gelten

```
CIRC_x_TYPE='ppp'  
CIRC_x_PPP_TYPE='umts'
```

(wobei “x” einen gültigen Circuit-Index darstellt).

Standard-Einstellung: `OPT_UMTS='no'`

Beispiel: `OPT_UMTS='yes'`

**UMTS\_DEBUG** Sollen während der UMTS-Initialisierung zusätzliche Informationen auf der Boot-Konsole ausgegeben werden, muss man `UMTS_DEBUG` auf ‘yes’ setzen.

Standard-Einstellung: `UMTS_DEBUG='no'`

Beispiel: `UMTS_DEBUG='yes'`

**UMTS\_PIN** Diese Variable enthält die Pin für die SIM-Karte. Erlaubt sind eine vierstellige Nummer oder das Wort ‘disabled’.

Standard-Einstellung: `UMTS_PIN='disabled'`

Beispiel: `UMTS_PIN='1234'`

**UMTS\_GPRS\_UMTS** Diese Variable definiert, welche Übertragungsart genutzt werden soll. Die erlaubten Werte sind `gprs` (nur GPRS), `umts` (nur UMTS) oder `both` (GPRS oder UMTS).

Standard-Einstellung: `UMTS_GPRS_UMTS='both'`

Beispiel: `UMTS_GPRS_UMTS='umts'`

**UMTS\_ADAPTER** Hier wird eingetragen, ob es sich bei dem UMTS-Gerät um eine PCMCIA-Karte (Wert `pcmcia`), einen USB-Adapter (Wert `usbstick`), um ein per USB-Kabel angeschlossenes Telefon (Wert `usbphone`), um einen auf dem GOBI1000-Chipsatz (Wert `gobi1000`) basierenden Adapter oder um einen auf dem GOBI2000-Chipsatz (Wert `gobi2000`) basierenden Adapter handelt.

Diese Variable ist optional. Bei Nichtvorhandensein der Variable werden nur die benötigten Dateien für einen USB-Adapter kopiert.

Standard-Einstellung: `UMTS_ADAPTER='usbstick'`

Beispiel: `UMTS_ADAPTER='usbphone'`

**Wichtig:** *Alle folgenden Variablen sind optional und nur notwendig wenn die automatische Erkennung versagt!*

**UMTS\_IDVENDOR** Diese Variable definiert die Hersteller-ID des UMTS-Geräts nach Einschalten des Adapters. Bei einem GOBI-Chipsatz ist die Angabe nötig.

Beispiel: `UMTS_IDVENDOR='12d1'`

**UMTS\_IDDEVICE** Diese Variable definiert die Produkt-ID des UMTS-Geräts nach Einschalten des Adapters. Bei einem GOBI-Chipsatz ist die Angabe nötig.

Beispiel: `UMTS_IDDEVICE='1446'`

**UMTS\_IDVENDOR2** Diese Variable definiert die Hersteller-ID des UMTS-Geräts nach Initialisierung des Adapters. Die Angabe ist nur notwendig, wenn sich diese ID nach der Initialisierung ändert. Bei einem GOBI-Chipsatz ist die Angabe nötig.

Beispiel: `UMTS_IDVENDOR2='12d1'`

**UMTS\_IDDEVICE2** Diese Variable definiert die Produkt-ID des UMTS-Geräts nach Initialisierung des Adapters. Die Angabe ist nur notwendig, wenn sich diese ID nach der Initialisierung ändert. Bei einem GOBI-Chipsatz ist die Angabe nötig.

Beispiel: `UMTS_IDDEVICE2='1436'`

**UMTS\_DRV** Diese Variable definiert den Treiber zum Ansteuern des Adapters. Wenn sie fehlt, wird `usbserial` angenommen.

Beispiel: `UMTS_DRV='option'`

**UMTS\_SWITCH** Diese Variable definiert Parameter für `usb-modeswitch`<sup>22</sup> zum Initialisieren des Modems. Es sollten bis auf wenige Ausnahmen alle auf der Webseite genannten Modems automatisch erkannt werden.

Beispiel: `UMTS_SWITCH='-v 0x0af0 -p 0x6971 -M 555...000 -s 10'`

**UMTS\_DEV** Bei Problemen kann hier die Datenschnittstelle für den PPP-Dämon angegeben werden. Für die Adapter sind das meist folgende:

<i>Adapter-Typ</i>	<i>Gerät</i>
<code>ttyUSB0</code>	usbstick
<code>ttyS2</code>	pcmcia
<code>ttyACM0</code>	usbphone

**UMTS\_CTRL** Einige Adapter haben mehrere Schnittstellen, über die das Modem gesteuert wird. Ist nur eine vorhanden können Statusinformationen nur im 'Offline'-Zustand ausgelesen werden. Bei einer Option Fusion UMTS Quad lautet die Schnittstelle beispielsweise `ttyUSB2`. Diese zusätzliche Schnittstelle kann hier angegeben werden.

Beispiel: `UMTS_CTRL='ttyUSB2'`

#### 4.23.2. UMTS-Circuit-Konfiguration

**CIRC\_x\_UMTS\_DIALOUT** Diese Variable definiert die zu wählende Nummer zum Herstellen der Verbindung.

Standard-Einstellung: `CIRC_x_UMTS_DIALOUT='*99***1\#'`

<sup>22</sup>siehe [http://www.draisberghof.de/usb\\_modeswitch/](http://www.draisberghof.de/usb_modeswitch/)

<i>Anbieter</i>	<i>APN</i>	<i>Benutzername</i>	<i>Passwort</i>
T-Mobile	internet.t-mobile	beliebig	beliebig
Vodafone	web.vodafone.de	beliebig	beliebig
E-Plus	internet.eplus.de	eplus	gprs
O2 (Vertragskunden)	internet	beliebig	beliebig
O2 (Prepaid-Kunden)	pinternet.interkom.de	beliebig	beliebig
Alice	internet.partner1	beliebig	beliebig

Tabelle 4.22.: Einwahldaten einiger deutscher Netzbetreiber/Provider

**CIRC\_x\_UMTS\_APN** Diese Variable definiert den Namen des zu nutzenden Access Points.

Standard-Einstellung: `CIRC_x_UMTS_APN='web.vodafone.de'`

Für einige deutsche Netzbetreiber bzw. Provider können die Einwahldaten (die über die Variablen `CIRC_x_UMTS_APN`, `CIRC_x_PPP_USERID` und `CIRC_x_PPP_PASSWORD` konfiguriert werden) Tabelle 4.22 entnommen werden.<sup>23</sup>

## 4.24. USB - Support für USB-Geräte

**OPT\_USB** Hier wird die grundsätzliche Unterstützung von USB-Geräten ein- beziehungsweise ausgeschaltet. Erst wenn hier 'yes' eingetragen wird, können USB-Geräte überhaupt verwendet werden. Sollten Sie also in der `base.txt` ein USB-Gerät ausgewählt haben, so müssen Sie hier zwingend 'yes' eintragen. Andernfalls wird das Gerät nicht verwendet. Mit der Aktivierung ist auch der Support für USB Sticks, externen Laufwerken und Tastaturen eingeschaltet.

Standard-Einstellung: `OPT_USB='no'`

**USB\_EXTRA\_DRIVER\_N** Anzahl der zusätzlich zu ladenden Treiber.

Standard-Einstellung: `USB_EXTRA_DRIVER_N='0'`

**USB\_EXTRA\_DRIVER\_x** Treiber der geladen werden soll.

Mögliche Werte im Moment

- `printer` - Unterstützung für USB-Drucker
- `belkin_sa` - USB Belkin Serial converter
- `cyberjack` - REINER SCT cyberJack pinpad/e-com USB Chipcard Reader
- `digi_acceleport` - Digi AccelePort USB-2/USB-4 Serial Converter
- `empeg` - USB Empeg Mark I/II
- `ftdi_sio` - USB FTDI Serial Converter
- `io_edgeport` - Edgeport USB Serial
- `io_ti` - Edgeport USB Serial
- `ipaq` - USB PocketPC PDA

<sup>23</sup>Quelle: <http://www.teltarif.de/mobilfunk/internet/einrichtung.html>

- ir-usb - USB IR Dongle
- keyspan - Keyspan USB to Serial Converter
- keyspan\_pda - USB Keyspan PDA Converter
- kl5kusb105 - KLSI KL5KUSB105 chipset USB->Serial Converter
- kobil\_sct - KOBIL USB Smart Card Terminal (experimental)
- mct\_u232 - Magic Control Technology USB-RS232 converter
- omninet - USB ZyXEL omni.net LCD PLUS
- pl2303 - Prolific PL2303 USB to serial adaptor
- visor - USB HandSpring Visor / Palm OS
- whiteheat - USB ConnectTech WhiteHEAT

Standard-Einstellung: `USB_EXTRA_DRIVER_x=""`

**USB\_EXTRA\_DRIVER\_x\_PARAM** Parameter für den zusätzlichen Treiber. Im Normalfall muss hier nichts eingegeben werden.

Standard-Einstellung: `USB_EXTRA_DRIVER_x_PARAM=""`

**USB\_MODEM\_WAITSECONDS** Standard-Einstellung: `USB_MODEM_WAITSECONDS='21'`

Leider braucht das Speedtouch USB Modem eine halbe Ewigkeit bis es bereit ist. In den meisten Fällen reichen die 21 Sekunden, die als Standardeinstellung genommen werden, für die Initialisierung aus. Manchmal hat man das Glück das man den Wert auch halbieren kann und das Speedtouch USB Modem bereits nach 10 Sekunden einsatzbereit ist, dann kann man hier halt 10 Sekunden eintragen. Wenn man Pech hat muss man den Wert erhöhen. Hier hilft leider nur probieren und austesten.

#### 4.24.1. Probleme mit USB-Geräten

Es kann bei einigen USB-Geräten zu Problemen kommen. Das kann verschiedene Ursachen haben, wie Beispielsweise der Treiber-Software oder dem USB-Controller.

#### 4.24.2. Hinweise zur Benutzung

Es ist darauf zu achten, dass die USB-Unterstützung hardwareseitig aktiviert ist. Insbesondere bei Onboard-USB-Kontrollern ist das wichtig. So wird z. B. ein WRAP ohne USB-Anschluss ausgeliefert. USB kann hier durch ein Zusatzmodul nachgerüstet werden und ist aus diesem Grund im BIOS standardmäßig deaktiviert.

#### 4.24.3. Mounten von USB-Geräten

Eingesteckte USB-Geräte werden zwar automatisch erkannt, müssen aber 'von Hand' sowohl an- als auch abgemeldet werden. Beim Einstecken z. B. eines USB-Stick wird dieser als SCSI-Device erkannt. Aus diesem Grund erfolgt der Zugriff über das Device `sd#` bei SuperFloppy-Geräten bzw. über `sd#<Partitionsnummer>` bei Geräten mit einer Partitionstabelle. USB-Sticks werden wie Festplatten behandelt, also bei zwei USB-Anschlüssen `sda1` und `sdb1` angesprochen. USB-Floppies hingegen werden durch `sda` bzw. `sdb` angesprochen, also ohne Angabe einer Partitionsnummer.

Somit kann ein USB-Stick durch das Kommando

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

nach /mnt gemountet werden. Analog dazu durch

```
mount /dev/sdb1 /mnt
```

für das zweite USB-Gerät. Die Geräte werden in der Reihenfolge des Einsteckens benannt, also erstes USB-Gerät = sda, zweites USB-Gerät = sdb etc. pp. Es lässt sich somit nicht fix definieren, welcher der USB-Ports welche 'Bezeichnung' hat, da diese von der Reihenfolge des Einsteckens der Geräte abhängt. Die Abmeldung der angemeldeten USB-Geräte erfolgt durch

```
umount /mnt
```

Bei gleichzeitiger Verwendung mehrerer USB-Geräte sollte es unbedingt vermieden werden, alles in ein Ziel zu mounten. Aus diesem Grund bietet es sich an, unterhalb von /mnt weitere Verzeichnisse anzulegen, in welche die Geräte dann gemountet werden können. Dies kann z. B. wie folgt erledigt werden:

```
mkdir /mnt/usba mkdir /mnt/usbb
```

Beim Mounten der Geräte werden dann diese Verzeichnisse als Ziel angegeben:

```
mount /dev/sda1 /mnt/usba mount /dev/sdb1 /mnt/usbb
```

Somit ist der Inhalt der USB-Geräte unter /mnt/usba bzw. /mnt/usbb zu finden. Die Abmeldung erfolgt dann durch

```
umount /mnt/usba umount /mnt/usbb
```

Wenn mehrere Partitionen je USB-Gerät existieren, müssen die Verzeichnisse unterhalb von /mnt entsprechend strukturiert werden.

### 4.25. VPN - Unterstützung virtueller privater Netzwerke

Dieses Paket erlaubt es, gesicherte Verbindungen zwischen privaten Netzwerken über öffentliche, aber unsichere Netzwerke aufzubauen.

#### 4.25.1. PPTP-Tunnel

PPTP<sup>24</sup> bietet eine Möglichkeit, einen privaten Kanal über ein öffentliches Netzwerk aufzubauen. Dabei wird der Tunnelaufbau und -abbau über ein spezielles TCP/IP-Kontrollprotokoll gesteuert. Die eigentlichen Nutzdaten werden in PPP-Paketen verpackt, die über einen GRE-Tunnel<sup>25</sup> geschickt werden.

In Österreich (und anderen europäischen Ländern) wird PPTP zusätzlich als Protokoll zwischen Router und DSL-Modem verwendet. Im Gegensatz zu PPPoE und PPPoA, die beide noch unterhalb der IP-Ebene arbeiten (Sicherheitsschicht, "Link Layer"), gibt es bei PPTP wie oben beschrieben zwei Datenströme. Somit benötigt man für DSL über PPTP im Gegensatz zu anderen DSL-Zugangsmethoden auch für die für PPTP reservierte Ethernet-Karte eine IP-Adresse. Die ist je nach Provider entweder fest vorgegeben oder muss via DHCPv4 konfiguriert werden. Mehr dazu steht in der Beschreibung der Variable `CIRC_x_PPP_PPTP_PEER`.

Ist man auf Grund eines DSL-Anschlusses oder einer veralteten VPN-Gegenstelle nicht gezwungen, PPTP zu nutzen, so wird davon abgeraten, PPTP als VPN-Lösung zu verwenden.

---

<sup>24</sup>"Point-to-Point Tunneling Protocol", siehe RFC 2637

<sup>25</sup>"Generic Routing Encapsulation", ein Protokoll, welches beliebige andere Protokolle kapseln und über IP-Netzwerke transportieren kann, siehe RFC 2784

Die Verschlüsselung in PPTP gilt als geknackt<sup>26</sup>, so dass man über PPTP-Tunnel nicht sicherheitskritische Daten verschicken sollte. Für einen solchen Einsatzzweck bilden Tunnel auf der Basis von OpenVPN sicherlich die bessere Wahl.

### Ausgehende PPTP-Verbindungen

Generell werden ausgehende PPTP-Verbindungen als PPP-Circuits konfiguriert (siehe [Circuits vom Typ “ppp”](#) (Seite 225)), d. h. es gilt:

```
CIRC_x_TYPE='ppp'
```

Zusätzlich muss das OPT\_PPP\_PPTP aktiviert werden:

**OPT\_PPP\_PPTP** Diese Variable aktiviert die Unterstützung für PPTP. Damit auch tatsächlich eine PPTP-Verbindung genutzt werden kann, muss mindestens ein PPP-Circuit den Typ “pptp” besitzen, d. h. es muss zusätzlich gelten

```
CIRC_x_TYPE='ppp'
CIRC_x_PPP_TYPE='pptp'
```

(wobei “x” einen gültigen Circuit-Index darstellt).

Standard-Einstellung: OPT\_PPP\_PPTP='no'

Beispiel: OPT\_PPP\_PPTP='yes'

**CIRC\_x\_PPP\_PPTP\_TYPE** Diese Variable definiert, wer die PPP-Datenpakete in GRE-Paketen kapselt und über die Leitung schickt. Dies kann durch ein Benutzerprogramm (pptp) oder durch den Kern erfolgen. Mittels CIRC\_x\_PPP\_PPTP\_TYPE wird die Art und Weise der GRE-Paketerzeugung definiert, siehe hierzu Tabelle 4.23.

Wert	Beschreibung
kernel	Die PPP-Pakete werden direkt an den Linux-Kern gereicht, der daraus GRE-Pakete macht. Dadurch entfällt die Kommunikation mit einem zweiten Prozess und damit ein Menge Kopier- und Scheduling-Aufwand, was wiederum zu geringerer Prozessorlast führt.
daemon	Die Pakete werden durch den pptp-Dämon erzeugt; die Kommunikation zwischen pppd und pptp erfolgt asynchron. Das bedeutet, dass der Datenstrom mit Anfang- und Ende-Markern versehen wird, damit der pptp-Dämon die einzelnen Pakete auseinanderhalten kann. Aufgrund des zweiten Prozesses und der zusätzlichen Markierungen ist diese Methode aufwändiger als die Methode “kernel”.

Tabelle 4.23.: Arten der GRE-Paketerzeugung

<sup>26</sup>siehe <http://heise.de/-1701365>



Momentan ist “daemon” die einzige unterstützte Methode (und somit auch Standard, falls der Typ nicht angegeben wird). Eine Erweiterung des Pakets um das Nutzen des entsprechenden pptp-Kernel-Moduls steht noch aus.

Standard-Einstellung: `CIRC_x_PPP_PPTP_TYPE='daemon'`

**CIRC\_x\_PPP\_PPTP\_PEER** Hier wird die IP-Adresse der PPTP-Gegenstelle eingetragen.

Nutzt man PPTP für einen DSL-Internet-Zugang, muss dazu passend die IP-Adresse der fli4l-PPTP-Ethernet-Karte gewählt werden. In Tabelle 4.24 sind bekannte Konfigurationsvarianten aufgelistet.

Provider	lokale IP-Adresse (IP_NET_2)	entfernte IP-Adresse (CIRC_x_PPP_PPTP_PEER)
Telekom Austria (Österreich)	10.0.0.140/29	10.0.0.138
mxstream (Niederlande, Dänemark)	10.0.0.140/29	10.0.0.138
Inode xDSL (Österreich)	via DHCPv4	10.0.0.138

Tabelle 4.24.: Einstellungen für Provider, die PPTP nutzen

Für den Fall, dass DHCP zur Konfiguration der lokalen Netzwerk-Karte benötigt wird, ist das dhcp\_client-Paket zu installieren und ein entsprechender DHCPv4-Circuit für die jeweilige Ethernet-Karte (in der Regel eth1) einzurichten. Ein Beispiel für Inode xDSL findet sich am Ende des Abschnitts.

**CIRC\_x\_PPP\_PPTP\_REORDER\_TIMEOUT** Der PPTP-Client muss unter Umständen Pakete zwischenspeichern und umordnen. Normalerweise wartet er 0,3 Sekunden auf ein ausstehendes Paket. Mit dieser Variable kann man den Timeout zwischen 0.00 (gar nicht puffern) und 10.00 (max. 10 Sekunden warten) variieren. Die Zeiten müssen immer mit Punkt und zwei Nachkommastellen angegeben werden.

Standard-Einstellung: `CIRC_x_PPP_PPTP_REORDER_TIMEOUT='0.30'`

Beispiel: `CIRC_1_PPP_PPTP_REORDER_TIMEOUT='1.00'`

**CIRC\_x\_PPP\_PPTP\_LOGLEVEL** Mit dieser Variable kann konfiguriert werden, wieviel Ausgaben der PPTP-Client produziert. Möglich sind 0 (wenig), 1 (mittel) und 2 (viel).

Standard-Einstellung: `CIRC_x_PPP_PPTP_LOGLEVEL='1'`

Beispiel: `CIRC_1_PPP_PPTP_LOGLEVEL='2'`

### Eingehende PPTP-Verbindungen

Der fli4l kann auch konfiguriert werden, *eingehende* PPTP-Verbindungen anzunehmen, also als ein Server zu fungieren. Solche PPTP-Verbindungen werden ebenfalls als PPP-Circuit konfiguriert (siehe [Circuits vom Typ “ppp”](#) (Seite 225)), d. h. es gilt:

`CIRC_x_TYPE='ppp'`

Zusätzlich muss das `OPT_PPP_PPTP_SERVER` aktiviert werden:

**OPT\_PPP\_PPTP\_SERVER** Mit dieser Variable wird die Unterstützung für eingehende PPTP-Verbindungen aktiviert. Damit auch tatsächlich PPTP-Verbindungen angenommen werden können, muss mindestens ein PPP-Circuit den Typ “pptp-server” besitzen, d. h. es muss zusätzlich gelten

```
CIRC_x_TYPE='ppp'
CIRC_x_PPP_TYPE='pptp-server'
```

(wobei “x” einen gültigen Circuit-Index darstellt).

Standard-Einstellung: OPT\_PPP\_PPTP\_SERVER='no'

Beispiel: OPT\_PPP\_PPTP\_SERVER='yes'

Zu den allgemeinen Circuit-Variablen kommen die folgenden, für PPP-Circuits des Typs “pptp-server” spezifischen Variablen hinzu:

**CIRC\_x\_PPP\_PPTP\_SERVER\_LISTEN** Mit dieser Variable kann die IPv4-Adresse festgelegt werden, an welcher der PPTP-Server horcht. Wird diese Variable weggelassen, horcht der PPTP-Server an *allen* Schnittstellen des Routers.<sup>27</sup>

Mit Hilfe der hier konfigurierten Adresse wird im Falle von `PF_INPUT_ACCEPT_DEF='yes'` (Seite 60) bzw. `PF_OUTPUT_ACCEPT_DEF='yes'` (Seite 63) die Firewall in den INPUT- und OUTPUT-Ketten sowohl für das PPTP-Kontrollprotokoll auf TCP-Port 1723 als auch für die GRE-Pakete geöffnet. Fehlt diese Variable, wird die Firewall so konfiguriert, dass die Kontroll- und Daten-Pakete an *jeder* Adresse des PPTP-Servers empfangen werden können.

Beispiel: CIRC\_1\_PPP\_PPTP\_SERVER\_LISTEN='IP\_NET\_1\_ADDR'

**CIRC\_x\_PPP\_PPTP\_SERVER\_ALLOW\_FROM\_y** Dieses Array enthält eine Liste von IPv4-Netzadressen, für die ein Zugriff auf den PPTP-Server in der Firewall erlaubt wird. Mit Hilfe der hier konfigurierten Adressen wird im Falle von `PF_INPUT_ACCEPT_DEF='yes'` (Seite 60) bzw. `PF_OUTPUT_ACCEPT_DEF='yes'` (Seite 63) die Firewall in den INPUT- und OUTPUT-Ketten sowohl für das PPTP-Kontrollprotokoll auf TCP-Port 1723 als auch für die GRE-Pakete geöffnet. Fehlt dieses Array, wird die Firewall so konfiguriert, dass die Kontroll- und Daten-Pakete von bzw. nach *überall* akzeptiert werden.

Beispiel:

```
CIRC_1_PPP_PPTP_SERVER_ALLOW_FROM_N='3'
CIRC_1_PPP_PPTP_SERVER_ALLOW_FROM_1='IP_NET_1'
CIRC_1_PPP_PPTP_SERVER_ALLOW_FROM_2='10.1.2.0/24'
CIRC_1_PPP_PPTP_SERVER_ALLOW_FROM_3='{Labor}'
```

**CIRC\_x\_PPP\_PPTP\_SERVER\_SESSIONS** Diese Variable enthält die Anzahl der Verbindungen, die dieser PPTP-Server maximal gleichzeitig verwalten kann. Maximal werden 255 Tunnel unterstützt.<sup>28</sup>

<sup>27</sup>Dies entspricht der IPv4-Adresse 0.0.0.0.

<sup>28</sup>Diese Beschränkung resultiert daher, dass der verwendete PPTP-Dämon einen Adressbereich nur in einer Komponente einer IPv4-Adresse erlaubt, also z.B. “192.168.222.0-254”. Da eine Komponente nur die Werte 0-255 annehmen kann und der Wert 255 für die Broadcast-Adresse reserviert sind, resultiert daraus die genannte Beschränkung.

#### 4. Pakete

Standard-Einstellung: CIRC\_x\_PPP\_PPTP\_SERVER\_SESSIONS='100'

Beispiel: CIRC\_1\_PPP\_PPTP\_SERVER\_SESSIONS='200'

#### Beispiele

Beispiel 1 (Internet-Zugang über PPTP mit fester lokaler Adresse):

```
IP_NET_N='2'                # (mindestens) zwei Netze (LAN + PPTP)
IP_NET_1='192.168.6.0/24'    # lokales Netz, wie benötigt konfigurieren
IP_NET_1_DEV='eth0'          # lokales Netz hängt an erster Karte
IP_NET_2='10.0.0.140/29'     # unsere Adresse im PPTP-Netz
IP_NET_2_DEV='eth1'          # Internet-Modem hängt an zweiter Karte
#
OPT_PPP='yes'                # PPP-Circuits aktivieren
OPT_PPP_PPTP='yes'           # PPTP-Client-Circuits aktivieren
#
CIRC_N='1'
CIRC_1_NAME='DSL-mxstream'    # beliebig, aber eindeutig
CIRC_1_TYPE='ppp'             # das ist ein PPP-Circuit
CIRC_1_ENABLED='yes'
CIRC_1_NETS_IPV4_N='1'
CIRC_1_NETS_IPV4_1='0.0.0.0/0' # Default-Route ins Internet
CIRC_1_CLASS_N='1'
CIRC_1_CLASS_1='internet'     # Klasse für Internet-Anbindung
CIRC_1_UP='yes'               # beim Booten aktivieren
CIRC_1_TIMES='Mo-Su:00-24:0.0:Y'
CIRC_1_USEPEERDNS='yes'       # DNS-Server des Providers nutzen
CIRC_1_PPP_TYPE='pptp'        # PPTP-Client
CIRC_1_PPP_USERID='anonymer'  # Benutzername zur Authentifizierung
CIRC_1_PPP_PASSWORD='surfer'  # Passwort zur Authentifizierung
CIRC_1_PPP_PPTP_PEER='10.0.0.138' # Adresse des Internet-Modems im PPTP-Netz
#
CIRC_CLASS_N='1'
CIRC_CLASS_1='internet'      # Klasse aller Internet-Circuits
```

Beispiel 2 (Internet-Zugang über PPTP mit dynamisch zugewiesener lokaler Adresse):

```
IP_NET_N='2'                # (mindestens) zwei Netze (LAN + PPTP)
IP_NET_1='192.168.6.0/24'    # lokales Netz, wie benötigt konfigurieren
IP_NET_1_DEV='eth0'          # lokales Netz hängt an erster Karte
IP_NET_2='{DHCP-Inode}'      # PPTP-Netz, via DHCP konfiguriert
IP_NET_2_DEV='eth1'          # Internet-Modem hängt an zweiter Karte
#
OPT_DHCP_CLIENT='yes'        # DHCP-Circuits aktivieren
OPT_PPP='yes'                # PPP-Client-Circuits aktivieren
OPT_PPP_PPTP='yes'           # PPTP-Client-Circuits aktivieren
#
CIRC_N='2'                   # zwei Circuits: DHCP und PPTP
#
CIRC_1_NAME='DHCP-Inode'     # beliebig, aber eindeutig
CIRC_1_TYPE='dhcp'           # das ist ein DHCP-Circuit
CIRC_1_ENABLED='yes'
```

#### 4. Pakete

```
CIRC_1_NETS_IPV4_N='1'           # hierüber soll die PPTP-Gegenstelle
CIRC_1_NETS_IPV4_1='10.0.0.138/32' # (= Internet-Modem) erreichbar sein
CIRC_1_DHCP_DEV='IP_NET_2_DEV'    # die PPTP-Ethernet-Karte
CIRC_1_UP='yes'                   # beim Booten aktivieren
#
CIRC_2_NAME='PPTP-Inode'          # beliebig, aber eindeutig
CIRC_2_TYPE='ppp'                 # das ist ein PPP-Circuit
CIRC_2_ENABLED='yes'
CIRC_2_PPP_TYPE='pptp'           # PPTP-Client
CIRC_2_PPP_USER='anonymer'        # Benutzername zur Authentifizierung
CIRC_2_PPP_PASS='surfer'          # Passwort zur Authentifizierung
CIRC_2_PPP_FILTER='yes'           # Datenverkehr-Filter aktivieren
CIRC_2_PPP_PPTP_PEER='10.0.0.138' # Adresse des Internet-Modems im PPTP-Netz
CIRC_2_NETS_IPV4_N='1'
CIRC_2_NETS_IPV4_1='0.0.0.0/0'    # Default-Route ins Internet
CIRC_2_USEPEERDNS='yes'           # DNS-Server des Providers nutzen
CIRC_2_HUP_TIMEOUT='600'          # nach 10 Minuten Inaktivität auflegen
CIRC_2_UP='yes'                   # beim Booten aktivieren
CIRC_2_DEPS='DHCP-Inode'          # PPTP benötigt DHCP-Konfiguration
```

Beispiel 3 (VPN-Client):

```
IP_NET_N='1'                     # (mindestens) ein (lokales) Netz
IP_NET_1='192.168.6.0/24'        # lokales Netz, wie benötigt konfigurieren
IP_NET_1_DEV='eth0'              # lokales Netz hängt an erster Karte
#
OPT_PPP='yes'                    # PPP-Circuits aktivieren
OPT_PPP_ETHERNET='yes'          # PPPoE-Client-Circuits aktivieren (DSL)
OPT_PPP_PPTP='yes'              # PPTP-Client-Circuits aktivieren (VPN)
#
CIRC_N='2'                       # zwei Circuits: PPPoE (Internet) und PPTP
#
CIRC_1_NAME='DSL-Telekom'        # beliebig, aber eindeutig
CIRC_1_TYPE='ppp'                # das ist ein PPP-Circuit
CIRC_1_ENABLED='yes'
CIRC_1_NETS_IPV4_N='1'
CIRC_1_NETS_IPV4_1='0.0.0.0/0'   # Default-Route ins Internet
CIRC_1_CLASS_N='1'
CIRC_1_CLASS_1='internet'        # Klasse für Internet-Anbindung
CIRC_1_UP='yes'                  # beim Booten aktivieren
CIRC_1_TIMES='Mo-Su:00-24:0.0:Y'
CIRC_1_USEPEERDNS='yes'          # DNS-Server des Providers nutzen
CIRC_1_PPP_TYPE='ethernet'       # PPPoE-Client
CIRC_1_PPP_USERID='anonymer'     # Benutzername zur Authentifizierung
CIRC_1_PPP_PASSWORD='surfer'     # Passwort zur Authentifizierung
CIRC_1_PPP_ETHERNET_TYPE='kernel' # Kernel soll PPPoE-Pakete packen
CIRC_1_PPP_ETHERNET_DEV='eth1'   # DSL-Modem hängt an zweiter Karte
#
CIRC_2_NAME='VPN-Firma'          # beliebig, aber eindeutig
CIRC_2_TYPE='ppp'                # das ist ein PPP-Circuit
CIRC_2_ENABLED='yes'
CIRC_2_NETS_IPV4_N='1'
CIRC_2_NETS_IPV4_1='10.11.12.0/24' # Firmennetz
```

#### 4. Pakete

```
CIRC_2_DEPS='internet/ipv4'      # Verbindung zur Firma benötigt
                                # IPv4-Internet
CIRC_2_UP='yes'                  # beim Booten aktivieren
CIRC_2_TIMES='Mo-Su:00-24:0.0:Y'
CIRC_2_PPP_TYPE='pptp'          # PPTP-Client
CIRC_2_PPP_USERID='mustermann'  # Benutzername zur Authentifizierung
CIRC_2_PPP_PASSWORD='geheim'   # Passwort zur Authentifizierung
CIRC_2_PPP_PPTP_PEER='192.0.2.1' # Adresse des PPTP-Servers der Firma
#
CIRC_CLASS_N='1'
CIRC_CLASS_1='internet'        # Klasse aller Internet-Circuits
```

Beispiel 4 (VPN-Server):

```
OPT_PPP='yes'                   # PPP-Circuits aktivieren
OPT_PPP_PPTP_SERVER='yes'      # PPTP-Server-Circuits aktivieren
OPT_PPP_PEERS='yes'            # zum Speichern der Anmeldedaten
PPP_PEER_N='1'                  # 1x Anmeldedaten hinterlegen
PPP_PEER_1_USERID='user'       # Benutzername vom Client
PPP_PEER_1_PASSWORD='pass'     # Passwort vom Client
PPP_PEER_1_CIRCUITS='pptp-eth1' # Anmeldedaten gelten für PPTP-Circuit
#
CIRC_N='1'
CIRC_1_NAME='pptp-eth1'        # beliebig, aber eindeutig
CIRC_1_TYPE='ppp'              # das ist ein PPP-Circuit
CIRC_1_ENABLED='yes'
CIRC_1_UP='yes'                # beim Booten aktivieren
CIRC_1_TIMES='Mo-Su:00-24:0.0:Y'
CIRC_1_PROTOCOLS='ipv4'       # IPv4 soll über die Verbindung laufen
CIRC_1_PPP_TYPE='pptp-server'  # PPTP-Server
CIRC_1_PPP_PEER_AUTH='yes'     # Client-Authentifizierung ist Pflicht
CIRC_1_PPP_COMP_MPPE='yes'     # benutze Verschlüsselung
CIRC_1_PPP_LOCALIP='192.168.222.1' # IP-Adresse des Servers
CIRC_1_PPP_REMOTEIP='192.168.222.2' # Start-IP-Adresse der Clients
CIRC_1_PPP_PPTP_SERVER_SESSIONS='10' # max. 10 Tunnel
```

#### 4.25.2. fastd-Tunnel

Mit fastd<sup>29</sup> steht eine schnelle und kleine Alternative zu bekannten VPN-Lösungen bereit. Ziele bei der Entwicklung waren folgende Punkte:

- sehr kleine Binärdatei (um unter OpenWRT auf Geräten mit sehr wenig Speicher eingesetzt werden zu können)
- austauschbare Krypto-Methoden
- Nutzung von UDP, um auch hinter NAT eingesetzt werden zu können
- Unterstützung von 1:1 und 1:n Szenarios

---

<sup>29</sup>Fast and Secure Tunnelling Daemon

In vielen Freifunk-Projekten ist `fastd` Bestandteil der auf Gluon basierenden Firmware. Während dort in der Regel „klar“ ist, was Client und Server ist, wird dies nicht durch das verwendete Protokoll bestimmt, sondern nur durch die Nutzung. Für `fastd` werden daher neben der Serverinstanz bei jedem beteiligten Kommunikationspartner ein oder mehrere sogenannte Peers definiert. Für die Konfiguration der jeweiligen Gegenstelle kehren sich damit die Rollen um: was auf der einen Seite `Serverdaemon` ist, muss auf der anderen Seite als Peer konfiguriert werden und umgekehrt.

### Generelle Einstellungen

**OPT\_FASTD** Diese Variable aktiviert den `fastd`. Um tatsächlich Verbindungen aufzubauen, müssen diese natürlich noch entsprechend konfiguriert werden.

Standard-Einstellung: `OPT_FASTD='no'`

Beispiel: `OPT_FASTD='yes'`

**FASTD\_SECRET** Setzt den geheimen Schlüssel dieser `fastd`-Instanz. Ein Schlüsselpaar kann beispielsweise mit dem Programm `fastd` erzeugt werden, welches auf dem Router oder auf einem beliebigen anderen Linux-Rechner laufen kann:

```
# fastd --generate-key
2016-01-06 18:54:13 +0100 --- Info: Reading 32 bytes from /dev/random...
Secret: d8dec7f65c89a39561ecde12623e8051d1d7c4286253b119f155e3fe169cd161
Public: e89e34e53c35bd6d750558a5e747fa72f25fbc922c86625b705ef1aa1865e32a
```

Wird diese Variable leer gelassen, erzeugt das Startscript ein Schlüsselpaar und legt den Inhalt in der Datei `/tmp/fastd.secret` ab, die man sich dann vom Router runter kopieren kann. Der `fastd` Service wird dann nicht gestartet!

Standard-Einstellung: `FASTD_SECRET=''`

Beispiel: `FASTD_SECRET='d8dec7f65c89a39561ecde12623e8051d1d7c4286253b119f155e3fe169cd161'`

## 4.26. WLAN - Wireless-LAN Unterstützung

Achten Sie in jedem Fall darauf, dass Sie beim Einsatz von PCI Karten ein Mainboard benutzen, was mindestens die PCI 2.2 Spezifikationen erfüllt. Auf älteren Mainboard die nur PCI 2.1 oder älter unterstützen kann es zu den unterschiedlichsten Fehler kommen. Entweder startet der Computer gar nicht (er lässt sich nicht einmal einschalten), oder die WLAN-Karte wird beim PCI Scan nicht gefunden.

WLAN-Karten werden in der `base.txt` `IP_NET_X_DEV` mit `wlanX` angesprochen. Wenn nur eine WLAN-Karte im System ist, hat diese also den Namen `wlan0`.

### 4.26.1. WLAN-Konfiguration

**OPT\_WLAN** Standard-Einstellung: `OPT_WLAN='no'`

Aktiviert das Wireless LAN Option Pack.

**WLAN\_REGDOMAIN** Mit dieser Variable kann man die Landesspezifischen Einstellungen anpassen. Gültige Werte sind ISO 3166-1 alpha-2 Ländercodes wie z.B. 'DE' In verschiedenen Ländern gelten verschiedene Vorgaben für die Kanalauswahl und Sendeleistungen.

**WLAN\_N** Anzahl der voneinander unabhängigen WLAN-Konfigurationen. Steht hier eine '1' so ist das Verhalten wie in früheren Versionen von fli4l.

**WLAN\_x\_MAC** MAC-Adresse der WLAN-Karte in dieser Schreibweise:

XX:XX:XX:XX:XX:XX

Jedes X ist ein Hex-Digit der Mac-Adresse der Karte, für die diese Konfiguration gelten soll. Sollte keine der hier eingetragenen Mac-Adressen zu einer Karte passen, so wird die Konfiguration `WLAN_1_*` auf diese Karte angewandt und es wird eine Warnmeldung ausgegeben, die auf den Umstand hinweist. Die Warnmeldung enthält die festgestellte MAC-Adresse der Karte. Diese ist in der Konfiguration einzutragen, damit auch das Web-Interface problemlos funktionieren kann.

**WLAN\_x\_MAC\_OVERRIDE** Ändert die MAC-Adresse der WLAN-Karte damit man als Client an ein WLAN mit MAC-Filter verbinden kann ohne dort den Filter anpassen zu müssen. Hilfreich bei WAN-Anbindungen, die z.B. auf die MAC-Adresse eines gelieferten WLAN-USB-Sticks gebunden sind.

**WLAN\_x\_ESSID** Die SSID ist der Name für das Funknetzwerk. Die auch "Network Name" genannte Zeichenfolge kann bis zu 32 Zeichen lang sein. Sie wird im AP eines WLAN konfiguriert und von allen Clients, die darauf Zugriff haben sollen, eingestellt. Auch bei Ad-Hoc muß die SSID auf allen teilnehmenden Nodes identisch sein.

**WLAN\_x\_MODE** Stellt den zu verwendenden WLAN-Modus der Karte ein.

Standard-Einstellung: `WLAN_x_MODE='ad-hoc'`

Mögliche Werte:

ad-hoc	für ein Funknetz ohne Access-Point
managed	gemanagertes Funknetz mit mehreren Zellen
master	die WLAN-Karte arbeitet als Access-Point

`WLAN_x_MODE='master'` funktioniert nur mit einem geeigneten WLAN-Treiber.

**WLAN\_x\_NOESSID** Ermöglicht das Abschalten der ESSID in den Beacon Frames. Nur möglich mit Treiber `hostap_*` und Firmware `>= 1.6.3` im `WLAN_MODE='master'`

Dieses Feature ist optional und muß manuell zur `config/wlan.txt` hinzugefügt werden.

**WLAN\_x\_CHANNEL** Setzt den Übertragungskanal des Netzwerks.

Standard-Einstellung: `WLAN_x_CHANNEL='1'`

Mögliche Werte: 1-13 und 36,40,44,48,52,56,60,64,100,104,108,112,116,120,124,128,132,136,140

Bitte lesen sie die Dokumentation Ihrer WLAN-Karte um herauszufinden, welche Kanäle in Ihrem Land erlaubt sind. Sollten sie hier einen nicht erlaubten Kanal einstellen, so sind sie alleine dafür verantwortlich. In Deutschland sind die Kanäle 1-13 im Frequenzband 2,4 GHz (Modi: b und g) erlaubt. Die Kanäle im Bereich 36-140 (siehe oben) sind im 5 GHz zulässig.

Desweiteren ist der Wert '0' erlaubt, falls `WLAN_x_MODE='managed'` gesetzt ist. Dadurch wird kein expliziter Kanal eingestellt, sondern der AP auf allen verfügbaren Kanälen gesucht. Man kann dem Kanal-Wert auch einen Buchstaben a,b oder g anhängen (z.B. 5g), welcher dann den gewünschten Betriebsmodus/Frequenzband auswählt.

Ein angehängtes 'n' oder 'N' selektiert bei entsprechenden WLAN-Karten die Nutzung von 802.11n. Kleingeschrieben bedeutet: 20 MHz Kanalbreite, grossgeschrieben: 40 MHz Kanalbreite.

Großschreibung bei a/b/g sorgt bei einigen (aktuell nur `ath_pci`) Treibern dafür, dass proprietäre WLAN-Turbos aktiviert werden. Diese Option ist experimentell und kann auch wieder entfernt werden.

**WLAN\_x\_RATE** Setzt die Übertragungsgeschwindigkeit des Netzwerks.

Standard-Einstellung: `WLAN_x_RATE='auto'`

Mögliche Werte: 1,2,5.5,11,auto - Angaben in Megabit/s je nach Karte können auch noch diese Raten ausgewählt werden: 6,9,12,18,24,36,48 und 54. Bei manchen 54 MBit-Karten kann die Rate nicht angegeben werden. Hier ist dann 'auto' einzutragen.

**WLAN\_x\_RTS** Aktiviert RTS/CTS Handshake. Diese Option ist in grossen Wlans mit vielen sendenden Clients nuetzlich wenn sich die Clients gegenseitig nicht hoeren koennen sondern nur den AP. Ist diese Option aktiviert sendet der Client vor jedem Sendevorgang ein RTS mit der Bitte um Erlaubnis zum Senden und bekommt ein CTS, die Erlaubnis zum Senden, vom AP zurueck. Damit weiss jeder Client dass ein Client sendet auch wenn er diesen Client nicht hoert. Hierdurch werden Kollisionen vermindert weil sicher gestellt ist dass immer nur ein Client sendet. Diese Option macht nur unter der oben beschriebenen Situation Sinn weil sie zusaetzlichen overhead hinzufuegt und somit die Gesamtbandbreite verringert. Durch die Verringerung von Kollisionen kann sich die Bandbreite jedoch wieder erhoehen.

Dieses Feature ist optional und muß manuell zur `config/wlan.txt` hinzugefügt werden.

**WLAN\_x\_ENC\_N (Überholt)** Legt die Anzahl der Wireless Encryption Key's fest (WEP).

Mögliche Werte: 0-4

**WLAN\_x\_ENC\_x (Überholt)** Setzt die Wireless Encryption Keys.

Mögliche Werte:

<code>XXXX-XXXX-XXXX-XXXX-XXXX-XXXX-XX</code>	128 Bit Hex-Key (X=0-F)
<code>XXXX-XXXX-XX</code>	64 Bit Hex-Key (X=0-F)
<code>s:&lt;5 Zeichen&gt;</code>	64 Bit
<code>s:&lt;6-13 Zeichen&gt;</code>	128 Bit
<code>P:&lt;1-64 Zeichen&gt;</code>	128 Bit

Das Verfahren der Key-Vergabe mit `s:Text` ist **nicht** mit der Passphrase der Windows-Treiber kompatibel. Hier bitte einen Hex-Key verwenden! Unter Windows wird der Hex-Key meist **ohne** die Bindestriche '-' verwendet. Die Angabe mittels `P:<Text>` ist kompatibel zur Passphrase der meisten Windows WLAN-Treiber (wenn nicht allen) aber **nur** im 128 Bit Modus. Linux erlaubt es, verschiedene Schlüssellängen zu mischen. Windows-Treiber jedoch in der Regel **nicht**!



**WLAN\_x\_ENC\_ACTIVE (Überholt)** Legt den aktiven Wireless Encryption Key fest.

Mögliche Werte: 1-4

Diese Variable ist aufzunehmen, wenn `WLAN_x_ENC_N > 0` gesetzt wird. Ansonsten optional.

**WLAN\_x\_ENC\_MODE (Überholt)** Aktiviert den Encryption Mode.

Mögliche Werte:

on/off      mit oder ohne Verschlüsselung  
open        nimmt auch unverschlüsselte Pakete an  
restricted   nimmt nur verschlüsselte Pakete an

Sinnvoller Wert: 'restricted'

Dieses Feature ist optional und muß manuell zur `config/wlan.txt` hinzugefügt werden. Ist die Variable nicht vorhanden, so wird als Default 'off' angenommen, wenn kein WEP-Key definiert ist und 'restricted' wenn mindestens ein Key definiert ist.

**WLAN\_x\_WPA\_KEY\_MGMT** Will man statt WEP-Verschlüsselung WPA verwenden, stellt man hier den gewünschten WPA-Modus ein. Momentan wird nur WPA-PSK unterstützt, also WPA mit einem Client und Access-Point vorab bekannten Schlüssel. Dieser Schlüssel sollte sorgfältig gewählt werden und nicht zu kurz sein, da er ansonsten auch anfällig gegen Wörterbuchattacken ist.

Unterstützt werden im *managed*-Mode alle vom Wpa-Supplcanten ([http://hostap.epitest.fi/wpa\\_supplc/](http://hostap.epitest.fi/wpa_supplc/)) und im *master*-Mode alle vom Hostapd (<http://hostap.epitest.fi/hostapd/>) unterstützten Karten.

Erfolgreich getestet wurden bereits Karten basierend auf den Chipsätzen von Atheros und vom hostap-Treiber unterstützte Karten (sowohl im managed als auch im master mode). Theoretisch ist auch noch Unterstützung für atmel-Karten und einige andere möglich. Hier müssen die Ersteller der entsprechenden Opts aber ihre Opt-Pakete noch entsprechend anpassen.

**WLAN\_x\_WPA\_PSK** Hier wird der Schlüssel angegeben, der zur Kommunikation zwischen Client und Access-Point verwendet werden soll. Dieser Schlüssel wird in Form einer Passphrase (eines Satzes) angegeben, die mindestens 8 Zeichen lang sein muß und bis zu 63 Zeichen lang sein kann. Folgende Zeichen werden unterstützt:

a-z A-Z 0-9 ! # \$ % & ( ) \* + , - . / : ; < = > ? @ [ \ ] ^ \_ ` { | } ~

**WLAN\_x\_WPA\_TYPE** Zur Auswahl stehen hier 1 für WPA1, 2 für den WPA2 (IEEE 802.11i) Modus und 3 für beide - der Client kann dann entscheiden ob er WPA1 oder WPA2 nutzen möchte. Wenn die WLAN Hardware den Standard unterstützt, so ist dem sicheren WPA2 Verfahren den Vorzug zu geben.

**WLAN\_x\_WPA\_ENCRYPTION** Die Verschlüsselungsprotokolle TKIP und die erweiterte Version CCMP (AES-CTR/CBC-MAC Protocol, manchmal auch nur AES genannt) stehen hier zur Verfügung. CCMP wird eventuell nicht von älterer WLAN-Hardware unterstützt. Es können auch beide gemeinsam angegeben werden.

**WLAN\_x\_WPA\_DEBUG (Experimentell)** Bei Problemen mit der WPA-Anbindung kann man diese Variable auf 'yes' setzen, um den zuständigen daemon zu umfangreicheren Ausgaben zu veranlassen. Diese kann man dann zur Diagnose der Probleme verwenden.

**WLAN\_x\_AP** Registriert diese Node bei einem Access-Point.

Hier ist die MAC-Adresse des Access-Points anzugeben. Wenn man bereits den WLAN-Mode “master” ausgewählt hat, ist dieser Eintrag leer zu lassen. Diese Option ist nur dann sinnvoll, wenn der fli4l den AP nicht von selber finden kann oder an einen bevorzugten Access-Point gebunden werden soll. Nur zum Einsatz in WLAN-Mode “managed” gedacht.

Dieses Feature ist optional und muß manuell zur config/wlan.txt hinzugefügt werden.

**WLAN\_x\_ACL\_POLICY** Policy der ACL.

Standard-Einstellung: `WLAN_x_ACL_POLICY='allow'`

Beschreibt eine Aktion, der die angegebenen MAC-Adressen unterliegen:

- deny Keine der aufgelisteten MAC-Adressen erhält Zugang
- allow Nur aufgelistete MAC-Adressen erhalten Zugang
- open Alle MAC-Adressen erhalten unabhängig vom Filter Zugang

Leider werden WLAN\_ACL's aktuell nur von einem Treiber sauber unterstützt: `hostap_*` Als Alternative bieten sich die in 3.0.x deutlich erweiterten Firewall-Möglichkeiten an.

**WLAN\_x\_ACL\_MAC\_N** AP-ACLs - Einschränkung der erlaubten WLAN-Stationen.

Standard-Einstellung: `WLAN_x_ACL_MAC_N='0'`

Eine Zahl größer 0 aktiviert die Access Control List (der MAC-Adressenfilter) und gibt die Anzahl der ACL-Einträge an. Die Access Control List ist eine Liste von MAC-Adressen, denen der Zugang zum Access Point (AP) erlaubt/verboten wird. Anzahl der Mac-Adressen, die definiert werden.

**WLAN\_x\_ACL\_MAC\_x** Mac-Adressen in der Form: 00:00:E8:83:72:92

**WLAN\_x\_DIVERSITY** Hiermit kann man einstellen, ob manuelle Antennen-Diversity aktiviert wird.

Standard-Einstellung: `WLAN_x_DIVERSITY='no'` (automatische Wahl)

**WLAN\_x\_DIVERSITY\_RX** Auswahl der Empfangsantenne.

Standard-Einstellung: `WLAN_x_DIVERSITY_RX='1'`

- 0 = Automatische Auswahl
- 1 = Antenne 1
- 2 = Antenne 2

**WLAN\_x\_DIVERSITY\_TX** Auswahl der Sendeantenne.

Standard-Einstellung: `WLAN_x_DIVERSITY_TX='1'`

**WLAN\_x\_WPS** Aktiviert den WPS-Support. Push-Button und PIN ist möglich. Es ist sinnvoll, WLAN\_WEBGUI zu aktivieren, es sei denn es ist nur die Steuerung per Commandline gewünscht.

Standard-Einstellung: `WLAN_x_WPS='no'`

**WLAN\_x\_PSKFILE** Bei aktiviertem PSKFILE können neben dem unter WLAN\_x\_WPA\_PSK konfigurierten Preshared Key auch weitere Client-bezogene Keys genutzt werden. Aktuell nutzt die Funktion WLAN\_x\_WPS dieses File um darüber konfigurierten Clients individuelle Keys zu geben.

Wird das File abgeschaltet sind auch bisher mit aktiviertem File verbundene WPS-Clients nicht mehr in der Lage mit dem AccessPoint zu verbinden.

WPS-Clients, die mit abgeschaltetem File verbunden wurden, sind davon nicht betroffen.

Standard-Einstellung: WLAN\_x\_PSKFILE='yes'

**WLAN\_x\_BRIDGE** Alternativ zur Angabe im Paket ADVANCED\_NETWORKING kann hier umgekehrt angegeben werden an welche Bridge das WLAN gebunden werden soll.

Beispiel: WLAN\_x\_BRIDGE='br0'

Achtung: Entweder in Advanced-Network oder hier angeben! **Nicht** an beiden Stellen!

### 4.26.2. Weboberfläche

Das Paket bringt außerdem eine Weboberfläche für den mini-httpd mit. Die Weboberfläche wird beim Setzen OPT\_HTTPD='yes' automatisch mit aktiviert.

### 4.26.3. Beispiele

#### Anbindung an einen Access Point via WPA

```
OPT_WLAN='yes'
WLAN_N='1'
WLAN_1_MAC='00:0F:A3:xx:xx:xx'
WLAN_1_ESSID='foo'
WLAN_1_MODE='managed'           # Anbindung an Access Point
WLAN_1_CHANNEL='1'
WLAN_1_RATE='auto'
#
# WPA Konfiguration
#
WLAN_1_ENC_N='0'                # kein WEP
WLAN_1_WPA_KEY_MGMT='WPA-PSK'  # WPA pre shared key
WLAN_1_WPA_TYPE='1'            # WPA 1
WLAN_1_WPA_ENCRYPTION='TKIP'
WLAN_1_WPA_PSK='Deine gute Passphrase (8-63 Zeichen)'
#
# irrelevant im WPA Kontext
#
WLAN_1_ENC_N='0'
WLAN_1_ENC_ACTIVE='1'
WLAN_1_ACL_POLICY='allow'
WLAN_1_ACL_MAC_N='0'
```

#### Access Point mit WPA2 Verschlüsselung

```
OPT_WLAN='yes'
WLAN_N='1'
```

#### 4. Pakete

```
WLAN_1_MAC='00:0F:A3:xx:xx:xx'
WLAN_1_ESSID='foo'
WLAN_1_MODE='master'           # Access Point
WLAN_1_CHANNEL='1g'           # Channel 1, Modus 'g' auf einer
                                # Atheros-Karte

WLAN_1_RATE='auto'
#
# WPA Konfiguration
#
WLAN_1_ENC_N='0'               # kein WEP
WLAN_1_WPA_KEY_MGMT='WPA-PSK' # WPA pre shared key
WLAN_1_WPA_TYPE='2'           # WPA 2
WLAN_1_WPA_ENCRYPTION='CCMP'
WLAN_1_WPA_PSK='Deine gute Passphrase (8-63 Zeichen)'
#
# MAC basierte Zugriffskontrolle auf AP
#
WLAN_1_ACL_POLICY='allow'
WLAN_1_ACL_MAC_N='0'
#
# irrelevant im WPA Kontext
#
WLAN_1_ENC_ACTIVE='1'
```

#### Access Point mit WEP Verschlüsselung

```
OPT_WLAN='yes'
WLAN_N='1'
WLAN_1_MAC='00:0F:A3:xx:xx:xx'
WLAN_1_ESSID='foo'
WLAN_1_MODE='master'           # Access Point
WLAN_1_CHANNEL='1'
WLAN_1_RATE='auto'
#
# WEP Konfiguration
#
WLAN_1_WPA_KEY_MGMT=''         # kein WPA
WLAN_1_ENC_N='4'               # 4 WEP-Keys
WLAN_1_ENC_1='...'
WLAN_1_ENC_2='...'
WLAN_1_ENC_3='...'
WLAN_1_ENC_4='...'
WLAN_1_ENC_ACTIVE='1'         # erster Schlüssel ist aktiv
#
# MAC basierte Zugriffskontrolle auf AP
#
WLAN_1_ACL_POLICY='allow'
WLAN_1_ACL_MAC_N='0'
#
# irrelevant für WEP Konfiguration
#
WLAN_1_WPA_TYPE='2'
WLAN_1_WPA_ENCRYPTION='CCMP'
```

```
WLAN_1_WPA_PSK='...'
```

#### 4.26.4. Virtual Accesspoint (VAP)(Experimentell)

Bestimmte WLAN-Karten (Treiber: ath\_pci, ath5k, ath9k, ath9k\_htc) können auf bis zu 4 virtuelle WLAN-Karten aufgeteilt werden. (VAP)

Die WLAN-Konfiguration der virtuellen AP kann beliebig sein bis auf folgende Bedingung: Gleich sein muss: Kanal und MAC-Adresse. Anhand der mehrfach verwendeten MAC-Adresse, wird die Karte identifiziert, die aufgesplittet werden soll. Bei mehreren verbauten Karten kann dies auch mehrfach gemacht werden.

Das Basis-Device wird weiterhin wlan0 heißen (bei einer WLAN-Karte). Bei VAP dann wlan0v2 usw. Zum binden an eine Bridge bitte hier WLAN\_x\_BRIDGE='br0' usw. verwenden!.

Das aktuelle Maximum ist: je nach Karte und Treiber bis zu 8x Master.

#### 4.26.5. Zeitgesteuertes ein- und ausschalten mit easycron

Mittels *easycron* (Seite 156), einem anderen Paket, kann das WLAN ein- und ausgeschaltet werden.

```
EASYCRON_N='2'
EASYCRON_1_CUSTOM = ''      # Jeden Abend um 24 Uhr ausschalten
EASYCRON_1_COMMAND = '/usr/sbin/wlanconfig.sh wlan0 down'
EASYCRON_1_TIME    = '* 24 * * *'

EASYCRON_2_CUSTOM = ''      # und um 8 Uhr wieder an.
EASYCRON_2_COMMAND = '/usr/sbin/wlanconfig.sh wlan0'
EASYCRON_2_TIME    = '* 8 * * *'
```

#### 4.26.6. Spendenhinweis

Durch die großzügige Spende von 2 Ralink 2500 basierten WLAN-Karten können WLAN-Karten mit dem RT25xx Chipsatz mit fli4l in den Modi ad-hoc und managed verwendet werden. Als Treiber ist in der base.txt hierzu rt2500 auszuwählen. Die Karten wurden gespendet von:

Computer Contor, Pilgrimstein 24a, 35037 Marburg

### 4.27. SRC - Das fli4l-Buildroot

Dieses Kapitel ist hauptsächlich für Entwickler interessant, die Binärprogramme oder Linux-Kernel für den fli4l übersetzen wollen. Wenn Sie fli4l nur als Router einsetzen und keine Pakete für den fli4l anbieten wollen, die eigene Binärprogramme benötigen, können Sie dieses Kapitel komplett überspringen.

Generell ist für die Übersetzung von Programmpaketen für den fli4l ein Linux-System erforderlich. Eine Übersetzung unter anderen Betriebssystemen (Microsoft Windows, OS X, FreeBSD etc.) wird *nicht* unterstützt.

Die Anforderungen an ein Linux-System zur fli4l-Entwicklung sind wie folgt:

- GNU gcc und g++ in der Version 2.95 oder neuer

- GNU gcc-multilib (je nach Hostsystem nötig)
- GNU binutils (enthält den Binder sowie andere, notwendige Programme)
- GNU make in der Version 3.81 oder neuer
- GNU bash
- libncurses5-dev für **fbr-make \*-menuconfig** (je nach Hostsystem nötig)
- die Programme sed, awk, which, flex, bison und patch
- die Programme makeinfo (Paket texinfo) und msgfmt (Paket gettext)
- die Programme tar, cpio, gzip, bzip2 und unzip
- die Programme wget, rsync, svn und git
- die Programme perl und python

Im Folgenden repräsentieren **fett** gedruckte Zeichen zu tätigende Eingaben, das  $\leftarrow$ -Zeichen steht für die Eingabetaste Ihrer Tastatur und schließt einzugebende Befehle ab.

#### 4.27.1. Eine Übersicht über die Quellen

Im **src**-Verzeichnis finden Sie folgende Unterverzeichnisse:

Verzeichnis	Inhalt
<b>fbr</b>	In diesem Verzeichnis befindet sich ein angepasstes Buildsystem, das auf dem Buildroot zur uClibc (aktuell in der Version 0.9.33.2) basiert. FBR steht hierbei für “fli4l-Buildroot”. Damit ist es möglich, alle auf dem fli4l verwendeten Programme (Kernel, Anwendungen und Bibliotheken) neu zu übersetzen.
<b>fli4l</b>	Dieses Verzeichnis enthält die fli4l-spezifischen Quellen, nach Paketen geordnet. Alle Quellen, die in diesem Unterverzeichnis enthalten sind, wurden entweder speziell für die Verwendung mit fli4l geschrieben oder zumindest stark angepasst.
<b>cross</b>	In diesem Verzeichnis befinden sich Skripte, mit denen die Cross-Compiler erstellt werden können, die für das Übersetzen von mkfli4l für diverse Plattformen benötigt werden.

#### 4.27.2. Übersetzen eines Programms für den fli4l

Im Unterverzeichnis “fbr” finden Sie das Skript **fbr-make**, das die Übersetzung aller Programme aus den Basispaketen für den fli4l-Router steuert. Dieses Skript kümmert sich um das Herunterladen und Übersetzen aller für den fli4l benötigten Binärdateien. Generell legt das Skript Dateien in dem Verzeichnis `~/fbr` ab; existiert dieses noch nicht, wird es angelegt. (Dieses Verzeichnis kann mit Hilfe der Umgebungsvariable **FBR\_BASEDIR** verändert werden, siehe unten.)

## 4. Pakete

*Hinweis:* Während des Übersetzungsvorgangs wird viel Platz benötigt (momentan etwa 900 MiB für die heruntergeladenen Archive und knapp 30 GiB für die Zwischenergebnisse und die resultierenden Kompilate). Stellen Sie somit sicher, dass Sie unterhalb von `~/fbr` über genug Platz verfügen! (Alternativ können Sie auch die `FBR_TIDY`-Option nutzen, siehe unten.)

Die Verzeichnisstruktur unterhalb von `~/fbr` ist wie folgt:

Verzeichnis	Inhalt
<code>fbr-&lt;branch&gt;-&lt;arch&gt;</code>	Hierhin wird das uClibc-Buildroot entpackt. <code>&lt;branch&gt;</code> steht hierbei für den Entwicklungszweig (z.B. <code>trunk</code> ), aus dem das FBR stammt. Ist der Ursprung des FBRs ein entpacktes <code>src</code> -Paket, wird <code>fbr-custom</code> benutzt. <code>&lt;arch&gt;</code> steht für die jeweilige Prozessorarchitektur (z.B. <code>x86</code> oder <code>x86_64</code> ). Mehr zu diesem Verzeichnis steht weiter unten.
<code>dl</code>	Hier werden die heruntergeladenen Archive gespeichert.
<code>own</code>	Hier können eigene FBR-Pakete abgelegt werden, die ebenfalls übersetzt werden sollen.

Unterhalb des Buildroot-Verzeichnisses `~/fbr/fbr-<branch>-<arch>/buildroot` sind die folgenden Verzeichnisse interessant:

Verzeichnis	Inhalt
<code>output/sandbox</code>	In diesem Verzeichnis gibt es für jedes FBR-Paket ein Unterverzeichnis, das die Dateien des FBR-Pakets nach dem Übersetzungsvorgang aufnimmt. In dem Verzeichnis <code>output/sandbox/&lt;paket&gt;/target</code> befinden sich dabei die Dateien, die für den fli4l-Router vorgesehen sind. In dem Verzeichnis <code>output/sandbox/&lt;paket&gt;/staging</code> hingegen befinden sich Dateien, die zum Übersetzen <i>anderer</i> FBR-Pakete, die dieses FBR-Paket benötigen, erforderlich sind.
<code>output/target</code>	In diesem Verzeichnis werden <i>alle</i> übersetzten Programme für den fli4l-Router abgelegt. Dieses Verzeichnis spiegelt somit die Verzeichnisstruktur auf dem fli4l-Router wider. Mit Hilfe von <code>chroot</code> kann man in dieses Verzeichnis wechseln und die übersetzten Programme ausprobieren. <sup>30</sup>

### Allgemeine Einstellungen

Die Arbeitsweise von `fbr-make` kann durch verschiedene Umgebungsvariablen beeinflusst werden:

---

<sup>30</sup>Dies ist an gewisse Voraussetzungen geknüpft, siehe hierzu den Abschnitt [“Testen eines übersetzten Programms”](#) (Seite 297).

#### 4. Pakete

Variable	Beschreibung
FBR	Gibt den Pfad zum FBR explizit an. Standardmäßig wird der Pfad <code>~/fbr/fbr-&lt;branch&gt;-&lt;arch&gt;</code> (s.o.) verwendet.
FBR_BASEDIR	Gibt den Basispfad zum FBR explizit an. Standardmäßig wird der Pfad <code>~/fbr</code> (s.o.) verwendet. Diese Variable wird ignoriert, falls die Umgebungsvariable FBR gesetzt wird.
FBR_DLDIR	Gibt das Verzeichnis an, das die Quellarchive enthält. Standardmäßig wird der Pfad <code>\${FBR}/../dl</code> (also z.B. <code>~/fbr/dl</code> ) verwendet.
FBR_BRANCH	Gibt explizit den Namen des Branches an, unter dem die Pakete unterhalb von <code>~/fbr</code> (s.o.) gebaut werden. Diese Variable wird ignoriert, falls die Umgebungsvariable FBR gesetzt wird.
FBR_CATEGORY	Gibt explizit den Namen der Category an, unter dem die Pakete unterhalb von <code>~/fbr</code> (s.o.) gebaut werden. Diese Variable wird ignoriert, falls die Umgebungsvariable FBR gesetzt wird.
FBR_OWNDIR	Gibt das Verzeichnis an, das die eigenen Pakete enthält. Standardmäßig wird der Pfad <code>\${FBR}/../own</code> (also z.B. <code>~/fbr/own</code> ) verwendet.
FBR_TIDY	Wenn diese Variable den Wert “y” enthält, werden Zwischenergebnisse, die während des Bauens der FBR-Pakete entstehen, unmittelbar nach der Installation in das Verzeichnis <code>output/target</code> gelöscht. Das spart viel Speicherplatz und ist eigentlich immer empfehlenswert, wenn man nach dem Bauen von Paketen nicht den Drang verspürt, in <code>output/build/...</code> hineinzuschauen. Falls diese Variable den Wert “k” enthält, werden nur die Zwischenergebnisse in den diversen Linux-Kernel-Verzeichnissen entfernt, weil dies verhältnismäßig viel Platz spart, ohne dass dadurch Funktionalität verloren geht. Alle anderen Belegungen (oder wenn die Variable gänzlich fehlt) sorgen dafür, dass alle Zwischenergebnisse erhalten bleiben.
FBR_ARCH	Diese Variable gibt die Prozessorarchitektur an, für die das FBR (bzw. einzelne FBR-Pakete) gebaut werden sollen. Fehlt sie, wird x86 angenommen. Die unterstützten Architekturen sind weiter unten zu finden.

Momentan unterstützt das FBR die folgenden Architekturen:

Architektur	Beschreibung
x86	Intel x86-Architektur (32-Bit), auch IA-32 genannt.
x86_64	AMD x86-64-Architektur (64-Bit), von Intel auch Intel 64 oder EM64T genannt.



### Übersetzen aller FBR-Pakete

Wenn Sie **fbr-make** mit dem Argument **world** ausführen, dauert es je nach verwendetem Rechner und verwendeter Internetanbindung mehrere Stunden, bis alle Quellarchive heruntergeladen und übersetzt worden sind.<sup>31</sup>

### Übersetzen des Toolchains

Wenn Sie **fbr-make** mit dem Argument **toolchain** ausführen, werden alle FBR-Pakete heruntergeladen und übersetzt, die für das Bauen der eigentlichen fli4l-Binärprogramme benötigt werden (also Übersetzer, Binder, uClibc-Bibliothek etc.). Normalerweise wird dieses Kommando nicht benötigt, da alle FBR-Pakete vom Toolchain abhängig sind und somit diese Toolchain-Programme ohnehin heruntergeladen und gebaut werden.

### Übersetzen eines einzelnen FBR-Pakets

Wollen Sie hingegen nur ein bestimmtes FBR-Paket übersetzen (etwa die Programme für ein selbst entwickeltes OPT), können Sie den Namen des FBR-Pakets bzw. die Namen mehrerer FBR-Pakete dem **fbr-make**-Programm mitgeben (etwa **fbr-make openvpn** zum Herunterladen und Übersetzen der OpenVPN-Programme). Dabei werden alle nötigen Abhängigkeiten ebenfalls heruntergeladen und übersetzt.

### Erneutes Übersetzen eines einzelnen FBR-Pakets

Möchten Sie ein bestimmtes FBR-Paket erneut übersetzen (warum auch immer), müssen Sie zuerst die Informationen im FBR über den vorher stattgefundenen Übersetzungsvorgang entfernen. Dazu können Sie den Befehl **fbr-make <paket>-clean** (z.B. **fbr-make openvpn-clean**) verwenden. Dabei werden die Informationen all jener FBR-Pakete, die von dem angegebenen FBR-Paket abhängig sind, ebenfalls zurückgesetzt, so dass sie beim nächsten **fbr-make world** ebenfalls neu übersetzt werden.

### Erneutes Übersetzen aller FBR-Pakete

Möchten Sie das komplette FBR neu übersetzen (z.B. weil Sie es als Benchmark-Programm für Ihr neues High-End-Entwicklersystem nutzen wollen ;-), können Sie mit Hilfe des Kommandos **fbr-make clean** nach der Bestätigung einer Sicherheitsabfrage alle Artefakte entfernen, die während des letzten FBR-Baus erzeugt worden sind.<sup>32</sup> Dies ist auch nützlich, um belegten Plattenspeicher freizugeben.

### 4.27.3. Testen eines übersetzten Programms

Ist ein Programm mit **fbr-make** übersetzt worden, kann es auf dem Entwicklungsrechner auch getestet werden. Ein solcher Test funktioniert natürlich nur, wenn die Prozessorarchitektur des Entwicklerrechners mit der Prozessorarchitektur des fli4ls, für welchen die Programme übersetzt werden sollen, übereinstimmt. (Es ist z.B. nicht möglich, **x86\_64-fli4l**-Programme auf einem **x86**-Betriebssystem auszuführen.) Ist diese Voraussetzung erfüllt, kann man mit

---

<sup>31</sup>Das Herunterladen der Quellarchive wird natürlich nur einmal durchgeführt, so lange Sie das FBR nicht aktualisieren und dadurch neuere Paketversionen andere Quellarchive benötigen.

<sup>32</sup>Es wird das gesamte Verzeichnis `~/fbr/fbr-<branch>-<arch>/buildroot/output` entfernt.

```
chroot ~/.fbr/fbr-<branch>-<arch>/buildroot/output/target /bin/sh
```

in das fli4l-Zielverzeichnis wechseln und dort das/die übersetzte(n) Programm(e) direkt ausprobieren. Beachten Sie jedoch bitte, dass Sie für **chroot** Administrator-Rechte benötigen und daher je nach Vorliebe und Systemkonfiguration die Dienste von **sudo** oder **su** in Anspruch nehmen müssen! Auch müssen Sie zumindest das FBR-Paket **busybox** übersetzt haben (via **fbr-make busybox**), damit Sie in der **chroot**-Umgebung eine Shell zur Verfügung haben. Ein kleines Beispiel:

```
$ sudo chroot ~/.fbr/fbr-trunk-x86/buildroot/output/target /bin/sh
Passwort:(Ihr Passwort)
```

```
BusyBox v1.22.1 (fli4l) built-in shell (ash)
Enter 'help' for a list of built-in commands.
```

```
# ls
THIS_IS_NOT_YOUR_ROOT_FILESYSTEM  mnt
bin                                opt
dev                                proc
etc                                 root
home                               run
img                                sbin
include                            share
lib                                 sys
lib32                              tmp
libexec                            usr
man                                 var
media                              windows
# bc --version
bc 1.06
Copyright 1991-1994, 1997, 1998, 2000 Free Software Foundation, Inc.
# echo "42 - 23" | bc
19
#
```

### 4.27.4. Entwanzen eines übersetzten Programms

Macht ein Programm auf dem fli4l Probleme, mit anderen Worten: es stürzt ab, dann hat man die Möglichkeit, den Programmzustand unmittelbar vor dem Absturz nachträglich zu analysieren (auch “Post-Mortem Debugging” genannt). Hierzu muss man zuerst in der Konfiguration des **base**-Pakets **DEBUG\_ENABLE\_CORE='yes'** aktivieren. Wird dann beim Absturz ein Speicherabbild in **/var/log/dumps/core.<PID>** generiert, wobei “PID” die Prozessnummer des abgestürzten Prozesses ist, dann kann man den Zustand des Programms auf einem Linux-Rechner mit einem voll übersetzten FBR folgendermaßen analysieren. Im folgenden Beispiel ist das zu analysierende Programm **/usr/sbin/collectd**, das sich mit einem SIGBUS verabschiedet hatte. Das Speicherabbild liegt dabei in **/tmp/core.collectd**.

```
fli4l@eisler:~$ .fbr/fbr-trunk-x86/buildroot/output/host/usr/bin/i586-linux-gdb
GNU gdb (GDB) 7.5.1
Copyright (C) 2012 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
```

#### 4. Pakete

```
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.  Type "show copying"
and "show warranty" for details.
This GDB was configured as "--host=x86_64-unknown-linux-gnu --target=i586-buildr
oot-linux-uclibc".
For bug reporting instructions, please see:
<http://www.gnu.org/software/gdb/bugs/>.
(gdb) set sysroot /project/fli4l/.fbr/fbr-trunk-x86/buildroot/output/target↵
(gdb) set debug-file-directory /project/fli4l/.fbr/fbr-trunk-x86/buildroot/outpu
t/debug↵
(gdb) file /project/fli4l/.fbr/fbr-trunk-x86/buildroot/output/target/usr/sbin/co
llectd↵
Reading symbols from /project/fli4l/.fbr/fbr-trunk-x86/buildroot/output/target/u
sr/sbin/collectd...Reading symbols from /project/fli4l/.fbr/fbr-trunk-x86/buildr
oot/output/debug/.build-id/8b/28ab573be4a2302e1117964edede2e54ebdbdf.debug...don
e.
done.
(gdb) core /tmp/core.collectd↵
[New LWP 2250]
[New LWP 2252]
[New LWP 2259]
[New LWP 2257]
[New LWP 2255]
[New LWP 2232]
[New LWP 2235]
[New LWP 2238]
[New LWP 2242]
[New LWP 2244]
[New LWP 2245]
[New LWP 2231]
[New LWP 2243]
[New LWP 2251]
[New LWP 2248]
[New LWP 2239]
[New LWP 2229]
[New LWP 2249]
[New LWP 2230]
[New LWP 2247]
[New LWP 2233]
[New LWP 2256]
[New LWP 2236]
[New LWP 2246]
[New LWP 2240]
[New LWP 2241]
[New LWP 2237]
[New LWP 2234]
[New LWP 2253]
[New LWP 2254]
[New LWP 2258]
[New LWP 2260]
Failed to read a valid object file image from memory.
Core was generated by `collectd -f'.
Program terminated with signal 7, Bus error.
```

#### 4. Pakete

```
#0 0xb7705f5d in memcpy ()
    from /project/fli4l/.fbr/fbr-trunk-x86/buildroot/output/target/lib/libc.so.0
(gdb) backtrace
#0 0xb7705f5d in memcpy ()
    from /project/fli4l/.fbr/fbr-trunk-x86/buildroot/output/target/lib/libc.so.0
#1 0xb768a251 in rrd_write (rrd_file=rrd_file@entry=0x808e930, buf=0x808e268,
    count=count@entry=112) at rrd_open.c:716
#2 0xb76834f3 in rrd_create_fn (
    file_name=file_name@entry=0x808d2f8 "/data/rrdtool/db/vm-fli4l-1/cpu-0/cpu-i
nterrupt.rrd.async", rrd=rrd@entry=0xacff2f4c) at rrd_create.c:727
#3 0xb7683d7b in rrd_create_r (
    filename=filename@entry=0x808d2f8 "/data/rrdtool/db/vm-fli4l-1/cpu-0/cpu-int
errupt.rrd.async", pdp_step=pdp_step@entry=10, last_up=last_up@entry=1386052459,
    argc=argc@entry=16, argv=argv@entry=0x808cf18) at rrd_create.c:580
#4 0xb76b77fd in srrd_create (
    filename=0xacff33f0 "/data/rrdtool/db/vm-fli4l-1/cpu-0/cpu-interrupt.rrd.asy
nc",
    pdp_step=10, last_up=1386052459, argc=16, argv=0x808cf18) at utils_rrdcreate
.c:377
#5 0xb76b78cb in srrd_create_thread (targs=targs@entry=0x808bab8)
    at utils_rrdcreate.c:559
#6 0xb76b7a8f in srrd_create_thread (targs=0x808bab8) at utils_rrdcreate.c:491
#7 0xb7763430 in ?? ()
    from /project/fli4l/.fbr/fbr-trunk-x86/buildroot/output/target/lib/libpthread
.so.0
#8 0xb775e672 in clone ()
    from /project/fli4l/.fbr/fbr-trunk-x86/buildroot/output/target/lib/libpthread
.so.0
(gdb) frame 1
#1 0xb768a251 in rrd_write (rrd_file=rrd_file@entry=0x808e930, buf=0x808e268,
    count=count@entry=112) at rrd_open.c:716
716     memcpy(rrd_simple_file->file_start + rrd_file->pos, buf, count);
(gdb) print (char*) buf
$1 = 0x808e268 "RRD"
(gdb) print rrd_simple_file->file_start
value has been optimized out
(gdb) list
711     if((rrd_file->pos + count) > old_size)
712     {
713         rrd_set_error("attempting to write beyond end of file");
714         return -1;
715     }
716     memcpy(rrd_simple_file->file_start + rrd_file->pos, buf, count);
717     rrd_file->pos += count;
718     return count;        /* mimmic write() semantics */
719 #else
720     ssize_t _sz = write(rrd_simple_file->fd, buf, count);
(gdb) list 700
695     * rrd_file->pos of rrd_simple_file->fd.
696     * Returns the number of bytes written or <0 on error. */
697
698     ssize_t rrd_write(
699         rrd_file_t *rrd_file,
```

```

700      const void *buf,
701      size_t count)
702  {
703      rrd_simple_file_t *rrd_simple_file = (rrd_simple_file_t *)rrd_file->
pvt;
704      #ifdef HAVE_MMAP
(gdb) print *(rrd_simple_file_t *)rrd_file->pvt.
$2 = {fd = 9, file_start = 0xa67d0000 <Address 0xa67d0000 out of bounds>,
      mm_prot = 3, mm_flags = 1}

```

Hier sieht man nach etwas “Wühlen”, dass sich in dem `rrd_simple_file_t`-Objekt ein ungültiger Zeiger befindet (“Address ... out of bounds”). Im weiteren Debugging-Verlauf wurde deutlich, dass ein gescheiterter `posix_fallocate`-Aufruf die Ursache für den Programmabsturz war.

Wichtig hierbei ist, dass *alle* anzugebenden Pfade voll qualifiziert sind (`/project/...`) und dass man auch keine “Abkürzungen” (etwa `~/...`) verwendet. Wenn man dies nicht beachtet, kann es passieren, dass `gdb` die Debug-Informationen zur Anwendung und/oder zu den verwendeten Bibliotheken nicht findet. Die Debug-Informationen sind nämlich aus Platzgründen nicht direkt in dem untersuchten Programm enthalten, sondern in einer separaten Datei unterhalb des Verzeichnisses `~/fbr/fbr-<branch>-<arch>/buildroot/output/debug/` gespeichert.

#### 4.27.5. Informationen über das FBR

##### Anzeige der Hilfe

Was `fbr-make` alles für Sie tun kann, können Sie sich mit dem Kommando `fbr-make help` ausgeben lassen.

##### Anzeige von Programminformationen

Sie können sich alle verfügbaren FBR-Pakete sowie deren Versionen anschauen, indem Sie das Kommando `fbr-make show-versions` nutzen:

```

$ fbr-make show-versions.
Configured packages

acpid 2.0.20
actctrl 3.25+dfsg1
add-days undefined
[...]

```

##### Anzeige von Bibliotheksabhängigkeiten

Mit Hilfe des Kommandos `fbr-make links-against <soname>` können Sie sich alle Dateien in `~/fbr/fbr-<branch>-<arch>/buildroot/output/target` anzeigen lassen, die gegen eine Bibliothek mit dem Bibliotheksnamen `soname` gebunden sind. Um beispielsweise alle Programme und Bibliotheken zu identifizieren, welche die `libm` (Bibliothek mit mathematischen Funktionen) verwenden, nutzen Sie das Kommando `fbr-make links-against libm.so.0`, da `libm.so.0` der Bibliotheksname der `libm`-Bibliothek ist. Eine mögliche Ausgabe ist:

## 4. Pakete

```
$ fbr-make links-against librrd_th.so.4↵
Executing plugin links-against
Files linking against librrd_th.so.4
collectd usr/lib/collectd/rrdcached.so
collectd usr/lib/collectd/rrdtool.so
rrdtool usr/bin/rrdcached
```

Dabei steht in der ersten Spalte der Paketname und in der zweiten der (relative) Pfad zu der Datei, die gegen die angegebenen Bibliothek gebunden ist.

Um den Bibliotheksnamen für eine Bibliothek herauszufinden, können Sie `readelf` wie folgt nutzen:

```
$ readelf -d ~/.fbr/fbr-trunk-x86/buildroot/output/target/lib/libm-0.9.33.2.so |↵
> grep SONAME↵
0x0000000e (SONAME)                Library soname: [libm.so.0]
```

### Anzeige von Versionsänderungen

(Nur) für fli4l-Team-Entwickler mit Schreibzugriff auf das fli4l-SVN-Repository ist das Kommando `fbr-make version-changes` interessant. Es listet alle FBR-Pakete auf, deren Version lokal modifiziert wurde, deren Version in der Arbeitskopie also von der Repository-Version abweicht. Damit kann der Entwickler sich einen Überblick über aktualisierte FBR-Pakete verschaffen, etwa bevor er die Änderungen ins Repo schreibt. Eine mögliche Ausgabe ist:

```
$ fbr-make version-changes↵
Executing plugin version-changes
Package version changes
KAMAILIO: 4.0.5 --> 4.1.1
```

Hier sieht man sofort, dass das kamailio-FBR-Paket von der Version 4.0.5 auf die Version 4.1.1 aktualisiert worden ist.

### 4.27.6. Ändern der FBR-Konfiguration

#### Rekonfiguration des FBRs

Mit Hilfe des Kommandos `fbr-make buildroot-menuconfig` ist es zum einen möglich, die zu übersetzenden FBR-Pakete auszuwählen. Das ist nützlich, wenn Sie andere FBR-Pakete für den fli4l übersetzen möchten, die standardmäßig nicht aktiviert sind, aber im uClibc-Buildroot integriert sind, oder wenn Sie eigene FBR-Pakete aktivieren wollen. Zum anderen können andere, globale Eigenschaften des FBRs verändert werden, etwa die Version des verwendeten GCC-Compilers. Beim erfolgreichen Beenden des Konfigurationsmenüs wird die neue Konfiguration im Verzeichnis `src/fbr/buildroot/.config` gespeichert.

Beachten Sie jedoch bitte, dass solche Änderungen der Toolchain-Konfiguration offiziell *nicht* unterstützt werden, weil die resultierenden Binärprogramme mit hoher Wahrscheinlichkeit inkompatibel mit der offiziellen fli4l-Distribution werden. Wenn Sie also Binärprogramme für Ihr eigenes OPT benötigen und dieses OPT veröffentlichen wollen, sollten Sie keine Toolchain-Einstellung verändern!

### Rekonfiguration der uClibc-Bibliothek

Mit dem Kommando `fbr-make uclibc-menuconfig` kann die Funktionalität der verwendeten uClibc-Bibliothek verändert werden. Beim erfolgreichen Beenden des Konfigurationsmenüs wird die neue Konfiguration in `src/fbr/buildroot/package/uclibc/uclibc.config` gespeichert.

**Wie im letzten Abschnitt gilt auch hier: Eine Änderung ist mit hoher Wahrscheinlichkeit nicht kompatibel mit der offiziellen fli4l-Distribution und wird somit nicht unterstützt!**

### Rekonfiguration der Busybox

Mit Hilfe des Kommandos `fbr-make busybox-menuconfig` kann die Busybox in ihrer Funktionalität angepasst werden. Beim erfolgreichen Beenden des Konfigurationsmenüs wird die neue Konfiguration in `src/fbr/buildroot/package/busybox/busybox-<Version>.config` gespeichert.

**Auch hier gilt: Eine Änderung ist höchstwahrscheinlich nicht kompatibel mit der offiziellen fli4l-Distribution und wird somit nicht unterstützt! Allenfalls das Ergänzen der Busybox um neue Applets ist problemlos, solange Sie die so modifizierte Busybox nur auf Ihren fli4l-Router einsetzen (und nicht vom Nutzer Ihres OPTs den Einsatz einer derart modifizierten Busybox verlangen).**

### Rekonfiguration der Linux-Kernelpakete

Mit `fbr-make linux-menuconfig` bzw. `fbr-make linux-<version>-menuconfig` kann die Konfiguration aller aktivierten Kernel-Pakete bzw. eines bestimmten Kernel-Pakets vorgenommen werden. Beim erfolgreichen Beenden des Konfigurationsmenüs wird die neue Konfiguration in `src/fbr/buildroot/linux/linux-<version>/dot-config-<arch>` gespeichert.<sup>33</sup>

**Wie im letzten Abschnitt gilt auch hier: Eine Änderung ist höchstwahrscheinlich nicht kompatibel mit der offiziellen fli4l-Distribution und wird somit nicht unterstützt! Allenfalls das Ergänzen des Linux-Kernels um neue Module ist problemlos, solange Sie den so modifizierten Kernel nur auf Ihren fli4l-Router einsetzen (und nicht vom Nutzer Ihres OPTs den Einsatz eines derart modifizierten Kernels verlangen).**

#### 4.27.7. Aktualisierung des FBRs

Jedem der beschriebenen Kommandos geht eine Prüfung des FBRs auf Aktualität voraus. Wird eine Diskrepanz zwischen den Quellen, in denen sich `fbr-make` befindet (also entpacktes `src`-Paket oder SVN-Arbeitskopie) und dem FBR in `~/fbr/fbr-<branch>-<arch>/buildroot` entdeckt, wird letzteres auf den neuesten Stand gebracht. Dabei werden neu dazugekommene

<sup>33</sup>Dies gilt nur für den Standard-Kernel. Für Varianten eines Kernelpakets wird stattdessen eine `diff`-Datei in `src/fbr/buildroot/linux/linux-<version>/linux-<version>_<variante>/dot-config-<arch>.diff` abgelegt.

FBR-Pakete integriert sowie alte, nicht mehr enthaltene FBR-Pakete gelöscht. Auch die Konfigurationen werden verglichen: FBR-Pakete mit veränderter Konfiguration sowie alle davon abhängigen FBR-Pakete werden neu gebaut. Dies stellt sicher, dass das FBR auf Ihrem Computer immer dem der fli4l-Entwickler entspricht (mit Ausnahme Ihrer eigenen FBR-Pakete unterhalb von `~/.fbr/own/`). **Das bedeutet jedoch auch, dass Änderungen am offiziellen Teil der Buildroot-Konfiguration bei der nächsten Aktualisierung verloren gehen!** Auch deshalb ist eine Rekonfiguration des FBRs (s.o.) somit nicht zu empfehlen, zumindest nicht, wenn Sie mit `src`-Paketen anstatt mit SVN-Arbeitskopien arbeiten. (Bei der Aktualisierung einer SVN-Arbeitskopie werden Ihre lokalen Konfigurationsänderungen und die Änderungen im SVN-Repository zusammengeführt, so dass das Problem der verlorenen Konfiguration hier nicht auftritt.) Hingegen können Sie Ihre eigenen FBR-Pakete problemlos umkonfigurieren, ohne dass es bei einer Aktualisierung zu Datenverlusten kommt.

#### 4.27.8. Eigene Programme ins FBR einbinden

Die Übersetzung der einzelnen FBR-Pakete wird über kleine Makefiles gesteuert. Will man eigene FBR-Pakete entwickeln, so muss man ein Makefile sowie eine Konfigurationsbeschreibung unter `~/.fbr/own/<paket>/` ablegen. Wie diese aufgebaut sind und wie man daraus abgeleitet eigene Makefiles schreiben kann, wird in der Dokumentation des uClibc-Buildroots unter <http://buildroot.uclibc.org/downloads/manual/manual.html#adding-packages> ausführlich beschrieben.



## 5. Erzeugen der fli4l Archive/Bootmedien

Sind alle Konfigurationsarbeiten erledigt, können die fli4l Archive/Bootmedien, sei es eine bootfähige Compact-Flash, ein bootfähiges ISO-Image oder nur die zum Remote-Update benötigten Dateien, erstellt werden.

### 5.1. Erzeugen der fli4l Archive/Bootmedien unter Linux bzw. anderen Unix-Derivaten und Mac OS X

Dies geschieht mit Hilfe von Scripts (`.sh`), die im fli4l Wurzelverzeichnis zu finden sind.

```
mkfli4l.sh
```

Das Build-Script erkennt selbständig die unterschiedlichen [Bootvarianten](#) (Seite 29). Der einfachste Aufruf sieht unter Linux so aus:

```
sh mkfli4l.sh
```

Die Aktionen des Build-Scripts werden durch drei Mechanismen gesteuert:

- Konfigurationsvariable `BOOT_TYPE` aus der `<config>/base.txt`
- Konfigurationsdatei `<config>/mkfli4l.txt`
- Parameter des Build-Scripts

An Hand der Konfigurationsvariable `BOOT_TYPE` (Seite 29) entscheidet sich, welche Aktion des Build-Scripts ausgeführt wird:

- Erstellen eines bootfähigen fli4l CD-ISO-Images
- Bereitstellen der fli4l Dateien, zwecks Remote-Update
- Erzeugen der fli4l Dateien und direktes Remote-Update per SCP
- usw.

Die Beschreibung der Variablen der Konfigurationsdatei `<config>/mkfli4l.txt` finden Sie im Kapitel [Steuerungsdatei mkfli4l.txt](#) (Seite 313).

### 5.1.1. Kommandozeilenoptionen

Der letzte Steuerungsmechanismus ist das Anhängen von Optionsparametern an den Aufruf des Build-Script auf der Kommandozeile. Die Steuerungsmöglichkeiten entsprechen denen der Steuerungsdatei `mkfli4l.txt`. Die Angabe von Optionsparametern überschreiben die Werte aus der Steuerungsdatei. Aus Komfortgründen unterscheiden sich die Namen der Optionsparameter von den Namen der Variablen aus der Steuerungsdatei. Es existiert teilweise eine Kurz- und eine Langform:

Usage: `mkfli4l.sh [options] [config-dir]`

```
-c, --clean          cleanup the build-directory
-b, --build <dir>    set build-directory to <dir> for the fli4l-files
-h, --help           display this usage
--batch             don't ask for user input

config-dir          set other config-directory - default is "config"

--hdinstallpath <dir> install a pre-install environment directly to
                      usb/compact flash device mounted or mountable to
                      directory <dir> in order to start the real installation
                      process directly from that device
                      device either has to be mounted and to be writable
                      for the user or it has to be mountable by the user
                      Do not use this for regular updates!
```

#### \*\*\* Remote-Update options

```
--remoteupdate      remote-update via scp, implies "--filesonly"
--remoteremount      make /boot writable before copying files and
                      read only afterwards
--remoteuser <name>  user name for remote-update - default is "fli4l"
--remotehost <host>  hostname or IP of remote machine - default
                      is HOSTNAME set in [config-dir]/base.txt
--remotepath <path>  pathname on remote maschine - default is "/boot"
--remoteport <portnr> portnumber of the sshd on remote maschine
```

#### \*\*\* Netboot options (only on Unix/Linux)

```
--tftpbootpath <path>  pathname to tftpboot directory
--tftpbootimage <name> name of the generated bootimage file
--pxesubdir <path>     subdirectory for pxe files relative to tftpbootpath
```

#### \*\*\* Developer options

```
-u, --update-ver      set version to <fli4l_version>-rev<svn revision>
-v, --verbose         verbose - some debug-output
-k, --kernel-pkg      create a package containing all available kernel
                      modules and terminate afterwards.
                      set COMPLETE_KERNEL='yes' in config-directory/_kernel.txt
                      and run mkfli4l.sh again without -k to finish
```

## 5. Erzeugen der fli4l Archive/Bootmedien

<code>--filesonly</code>	create only fli4l-files - do not create a boot-media
<code>--no-squeeze</code>	don't compress shell scripts
<code>--rebuild</code>	rebuild mkfli4l and related tools; needs make, gcc

Eine HD-Vorinstallation einer passend formatierten (FAT16/FAT32) CompactFlash im USB-Cardreader oder eines USB-Sticks ist über die Option `--hdinstallpath <dir>` möglich. Dieses können Sie *auf eigenes Risiko* zur Installation auf eine CompactFlash oder einen USB-Stick benutzen. Hierbei werden auf die angegebene Partition die nötigen Dateien des fli4l kopiert. Sie rufen dazu zunächst im fli4l-Verzeichnis

```
sh mkfli4l.sh --hdinstallpath <dir>
```

auf. Dabei werden die fli4l Dateien auf eine CF-Card oder USB-Stick kopiert.

Um die nächsten Schritte ausführen zu können, sind folgende Voraussetzungen zu erfüllen:

- `chmod 777 /dev/brain`
- superuser-Rechte
- installiertes `syslinux`
- installiertes `fdisk`

Durch das Script erfolgt eine Kontrolle, ob dieser Datenträger tatsächlich ein USB-Laufwerk ist und die erste Partition eine FAT-Partition ist. Anschliessend werden der Bootloader und die nötigen Dateien auf den angegebenen Datenträger kopiert. Sie erhalten eine Meldung über den Erfolg oder Misserfolg.

Nach dem Build müssen Sie

```
syslinux --mbr /dev/brain

# make partition bootable using fdisk
#   p - print partitions
#   a - toggle bootable flag, specify number of fli4l partition
#       usually '1'
#   w - write changes and quit
fdisk /dev/brain

# install boot loader
syslinux -i /dev/brain
```

ausführen. Dann sollte die CF bzw. der USB-Stick bootfähig sein. Vergessen Sie nicht, den Datenträger auszuhängen (via `umount`).

Als letzter Optionsparameter kann ein alternatives Konfigurationsverzeichnis übergeben werden. Das normale Konfigurationsverzeichnis heißt `config` und liegt direkt im fli4l Wurzelverzeichnis. An diesem Ort legen alle fli4l Pakete die Konfigurationsdateien ab. Möchte man mehr

als eine Konfiguration verwalten, so erstellt man sich ein weiteres Verzeichnis, z.B. `hd.conf`, legt dort eine Kopie der Konfigurationsdateien ab und verändert diese den Anforderungen entsprechend. Hier einige Beispiele:

```
sh mkfli4l.sh --filesonly hd.conf
sh mkfli4l.sh --no-squeeze config.test
```

### 5.2. Erzeugen der fli4l Archive/Bootmedien unter Windows

Es wird das Tool ‘AutoIt3’ verwendet (<http://www.autoitscript.com/site/autoit/>). Dieses ermöglicht eine ‘grafische’ Ausgabe, sowie Dialoge, mit denen die in den folgenden Abschnitten beschriebenen Variablen beeinflusst werden können.

`mkfli4l.bat`

Das Build-Programm erkennt selbständig die unterschiedlichen [Bootvarianten](#) (Seite 29).

Der Aufruf von ‘mkfli4l.bat’ kann direkt aus dem Windows Explorer erfolgen, wenn man keine optionalen Parameter verwenden möchte.

Die Aktionen des Build-Programms werden durch verschiedene Mechanismen gesteuert:

- Konfigurationsvariable `BOOT_TYPE` aus der `<config>/base.txt`
- Konfigurationsdatei `<config>/mkfli4l.txt`
- Parameter des Build-Programmes
- Interaktive Einstellung in der GUI

An Hand der Konfigurationsvariable `BOOT_TYPE` (Seite 29) entscheidet sich, welche Aktion das Build-Programm ausführt:

- Erstellen eines bootfähigen fli4l CD-ISO-Images
- Bereitstellen der fli4l Dateien, zwecks Remote-Update
- Erzeugen der fli4l Dateien und direktes Remote-Update per SCP
- HD-pre-install einer passend formatierten CF im Cardreader
- usw.

Die Beschreibung der Variablen der Konfigurationsdatei `<config>/mkfli4l.txt` finden Sie im Kapitel [Steuerungsdatei mkfli4l.txt](#) (Seite 313).

#### 5.2.1. Kommandozeilenoptionen

Ein weiterer Steuerungsmechanismus ist das Anhängen von Optionsparametern an den Aufruf des Build-Programms auf der Kommandozeile. Die Steuerungsmöglichkeiten entsprechen denen der Steuerungsdatei `mkfli4l.txt`. Die Angabe von Optionsparametern überschreiben die Werte aus der Steuerungsdatei. Aus Komfortgründen unterscheiden sich die Namen der Optionsparameter von den Namen der Variablen aus der Steuerungsdatei. Es existiert teilweise eine Kurz- und eine Langform:

Usage: mkfli4l.bat [options] [config-dir]

```
-c, --clean          cleanup the build-directory
-b, --build <dir>    sets build-directory to <dir> for the fli4l-files
-v, --verbose        verbose - some debug-output
    --filesonly      creates only fli4l-files - does not create a disk
    --no-squeeze     don't compress shell scripts
-h, --help           display this usage
```

```
config-dir           sets other config-directory - default is "config"
```

#### \*\*\* Remote-Update options

```
--remoteupdate      remote-update via scp, implies "--filesonly"
--remoteuser <name> user name for remote-update - default is "fli4l"
--remotehost <host> hostname or IP of remote machine - default
                    is HOSTNAME set in [config-dir]/base.txt
--remotepath <path> pathname on remote machine - default is "/boot"
--remoteport <portnr> portnumber of the sshd on remote machine
```

#### \*\*\* GUI-Options

```
--nogui            disable the config-GUI
--lang             change language
                    [deutsch|english|espanol|french|magyar|nederlands]
```

Als letzter Optionsparameter kann ein alternatives Konfigurationsverzeichnis übergeben werden. Das normale Konfigurationsverzeichnis heißt `config` und liegt direkt im fli4l Wurzelverzeichnis. An diesem Ort legen alle fli4l Pakete die Konfigurationsdateien ab. Möchte man mehr als eine Konfiguration verwalten, so erstellt man sich ein weiteres Verzeichnis, z.B. `hd.conf`, legt dort eine Kopie der Konfigurationsdateien ab und verändert diese den Anforderungen entsprechend. Hier einige Beispiele:

```
mkfli4l.bat hd.conf
mkfli4l.bat -v
mkfli4l.bat --no-gui config.hd
```

### 5.2.2. Konfigurationsdialog – Einstellung des Konfigurationsverzeichnis

Im Hauptfenster wird die Einstellung des Konfigurationsverzeichnis angezeigt und es kann ein Fenster geöffnet werden zur Auswahl des Konfigurationsverzeichnis.

Zu beachten ist, dass eine Änderung des 'Config-Dir' alle Optionen auf die Werte setzt, die in der dortigen [Steuerungsdatei 'mkfli4l.txt'](#) (Seite [313](#)) gesetzt bzw. als Kommandozeilenparameter übergeben wurden.

## 5. Erzeugen der fli4l Archive/Bootmedien

Findet mkfli4l.bat kein Verzeichnis fli4l-x.y.z\config oder in dem Verzeichnis keine Datei mit dem Namen 'base.txt' öffnet sich sofort das Fenster zur Auswahl des Konfigurationsverzeichnis. Dieses ermöglicht es auf einfache Weise im fli4l-Verzeichnis mehrere Konfigurationen zu verwalten.

Beispiel:

```
fli4l-x.y.z\config  
fli4l-x.y.z\config.fd  
fli4l-x.y.z\config.cd  
fli4l-x.y.z\config.hd  
fli4l-x.y.z\config.hd-erstellen
```

### 5.2.3. Konfigurationsdialog – allgemeine Einstellungen

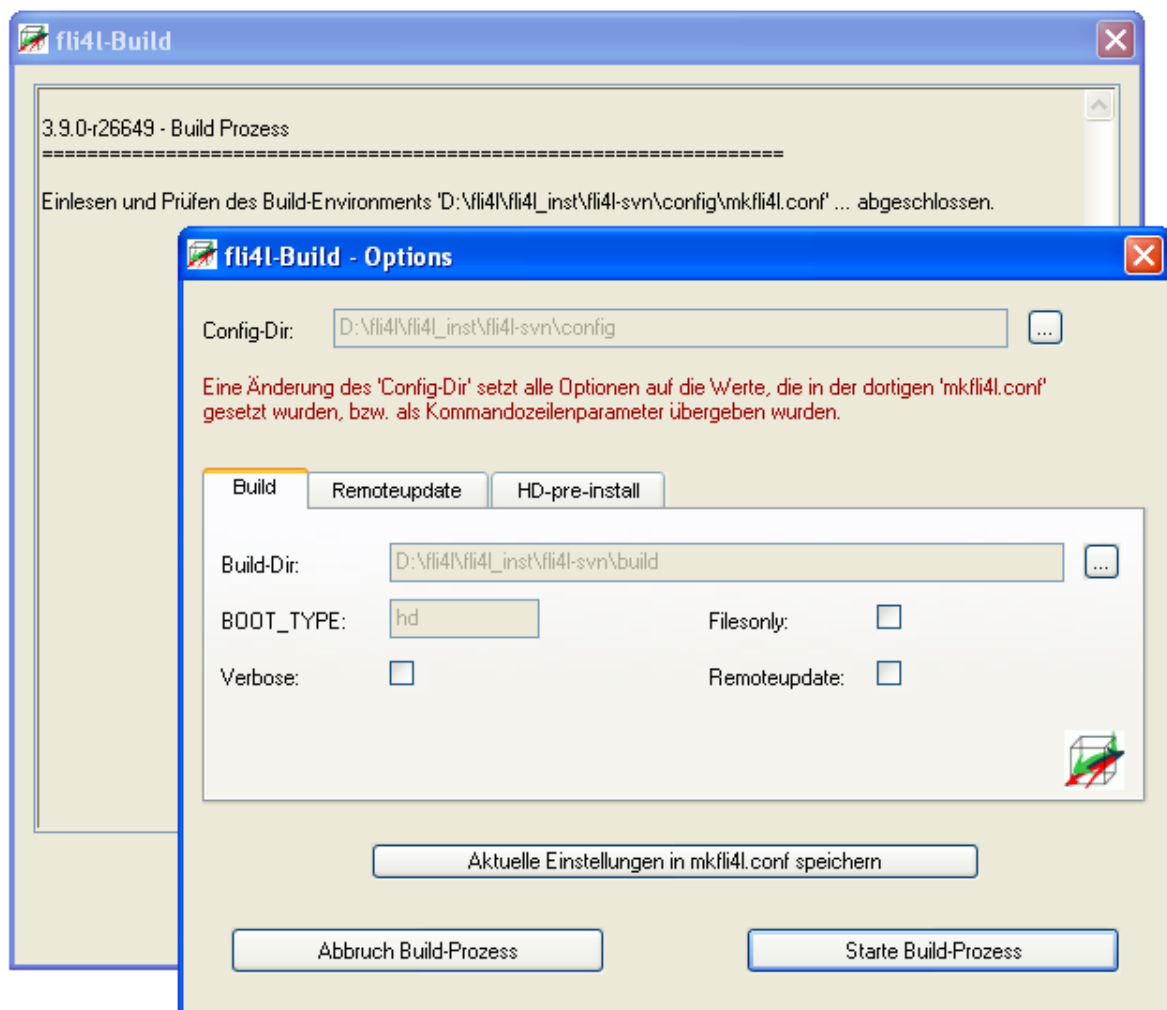


Abbildung 5.1.: Einstellungen

In diesem Dialog werden die Einstellungen für die Archiv/Bootmedienerstellung festgelegt:

## 5. Erzeugen der fli4l Archive/Bootmedien

- Build-Dir – Verzeichnis für die Archive/CD-Images/...
- BOOT\_TYPE – Anzeige des verwendeten/eingestellten BOOT\_TYPE – nicht änderbar
- Verbose – Aktivierung von zusätzlichen Ausgaben während der Erstellung
- Filesonly – es werden nur die Archive erstellt – kein bootmedium/kein Image
- Remoteupdate – Aktivierung des Remoteupdates per SCP

Mit der Schaltfläche **Aktuelle Einstellungen in mkfli4l.txt speichern** können die aktuell eingestellten Werte in der mkfli4l.txt gespeichert werden.

### 5.2.4. Konfigurationsdialog – Einstellungen für Remoteupdate

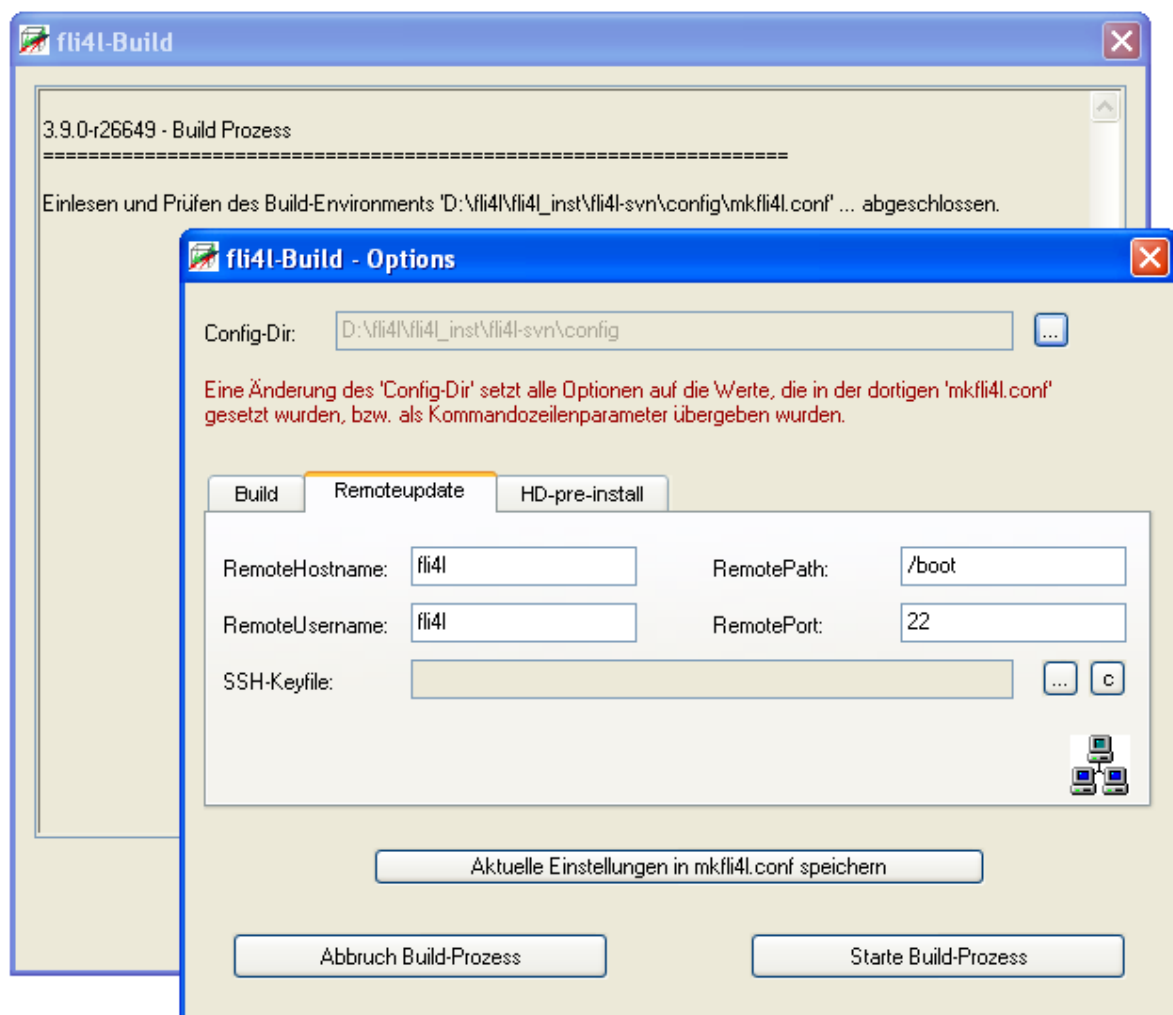


Abbildung 5.2.: Einstellungen für Remoteupdate

In diesem Dialog werden die Einstellungen für den Remoteupdate festgelegt:

## 5. Erzeugen der fli4l Archive/Bootmedien

- IP-Adresse oder Hostname
- Benutzername auf dem Remote-Host
- Remote-Pfad (default: /boot)
- Remote-Port (default: 22)
- zu verwendendes SSH-Keyfile (ppk-Format von Putty)

### 5.2.5. Konfigurationsdialog – Einstellungen für HD-pre-install

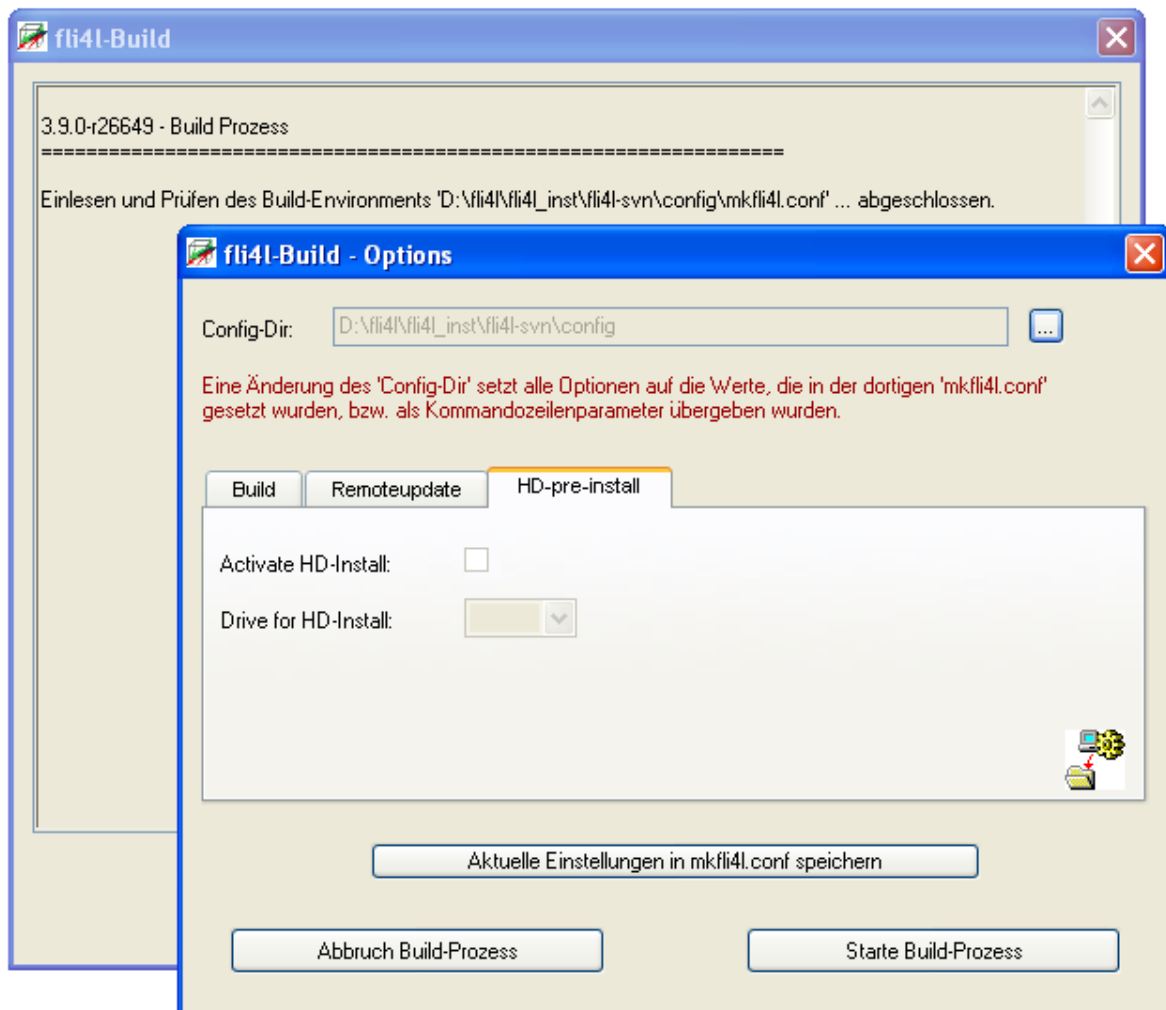


Abbildung 5.3.: Einstellungen für HD-pre-install

In diesem Dialog können die Optionen für den HD-pre-install auf einer entsprechend partitionierten und formatierten CompactFlash-Karte in einem USB-Reader eingestellt werden.

Mögliche Optionen:

- HD-pre-install aktivieren



- Laufwerksbuchstabe der CF-Karte

Hinweis zur Partitionierung und Formatierung der CF: Für eine HD-Installation nach TYP A (siehe dazu Paket HD) muss auf der CF eine primäre aktive und formatierte FAT-Partition vorhanden sein. Möchte man weiterhin auch eine Datenpartition benutzen, wird zusätzlich eine Linux-Partition, die mit dem Dateisystem ext3 formatiert ist, sowie die Datei `hd.cfg` auf der FAT-Partition benötigt (hierzu sollten unbedingt die Hinweise im Paket HD beachtet werden).

### 5.3. Steuerungsdatei `mkfli4l.txt`

Seit fli4l-Version 2.1.9 existiert die Steuerungsdatei `<config>/mkfli4l.txt`. Durch sie werden z.B. vom Standard abweichende Verzeichnisse übergeben. Die Steuerungsdatei hat einen ähnlichen Aufbau wie die normalen fli4l Konfigurationsdateien. Alle Konfigurationsvariablen sind hier optional, d.h. sie müssen nicht in der Konfigurationsdatei vorkommen oder können als Kommentar gekennzeichnet werden.

**BUILDDIR** Standardwert: `'build'`

Legt fest, in welchem Verzeichnis die fli4l Dateien erzeugt werden sollen. Ist die Variable undefiniert, setzt `mkfli4l` unter Windows `'build'` relativ zum fli4l Wurzelverzeichnis ein und meint damit also das Verzeichnis `build` im fli4l Wurzelverzeichnis:

`Pfad/fli4l-x.y.z/build`

Unter \*nix setzt `mkfli4l` `<config>/build` ein und legt damit die generierten Dateien zusammen mit der Konfiguration ab.

Die konfigurierten Pfade in **BUILDDIR** müssen der jeweiligen Logik von Windows oder \*unix entsprechen. Werden relative Pfade gesetzt, wird der Pfad durch den Buildprozess passend zu Windows oder \*unix konvertiert.

**VERBOSE** Standardwert: `VERBOSE='no'`

Mögliche Werte sind `'yes'` oder `'no'`. Steuert die *Geschwätzigkeit* des Build Prozesses.

**FILESONLY** Standardwert: `FILESONLY='no'`

Mögliche Werte `'yes'` oder `'no'`. Hiermit kann das Erstellen eines Boot-Mediums abgeschaltet werden, es werden also nur die Dateien erzeugt –

**REMOTEUPDATE** Standardwert: `REMOTEUPDATE='no'`

Mögliche Werte `'yes'` oder `'no'`. Aktiviert das automatische Übertragen der erstellten Dateien mittels SCP auf den Router. Dieses setzt ein installiertes Paket [SSHD](#) (Seite 261) mit aktiviertem `scp` voraus. Siehe dazu auch die folgenden Variablen.

**REMOTEHOSTNAME** Standardwert: `REMOTEHOSTNAME=""`

Gibt den Ziel-Hostnamen für den SCP Datentransfer an. Sollte kein Name angegeben sein, wird dieser der Variable [HOSTNAME](#) (Seite 28) entnommen.

**REMOTEUSERNAME** Standardwert: `REMOTEUSERNAME='fli4l'`

Username für den SCP Datentransfer.

**REMOTEPATHNAME** Standardwert: REMOTEPATHNAME= '/boot'

Ziel-Pfad für den SCP Datentransfer.

**REMOTEPORT** Standardwert: REMOTEPORT= '22'

Zielpport für den SCP Datentransfer.

**SSHKEYFILE** Standardwert: SSHKEYFILE=""

Hier kann man eine SSH-Keydatei für den SCP-Remoteupdate angeben. Es kann somit ein Update ohne Angabe eines Passwortes erfolgen.

**REMOTEREMOUNT** Standardwert: REMOTEREMOUNT= 'no'

Mögliche Werte 'yes' oder 'no'. Wird hier 'yes' gesetzt, wird ein eventuell Readonly eingehängtes Bootdevice /boot für das Remoteupdate Readwrite gemountet um das Remoteupdate möglich zu machen.

**TFTPBOOTPATH** Pfad an dem das Netboot-Image abgelegt wird.

**TFTPBOOTIMAGE** Name des Netboot-Images.

**PXESUBDIR** Unterverzeichnis für die PXE-Dateien relativ zu TFTPBOOTPATH.

**SQUEEZE\_SCRIPTS** Aktiviert bzw. deaktiviert das Squeezen (Kommprimieren) von Skripten. Das Komprimieren eines Skripts mit Squeeze entfernt alle Kommentare und Zeileneinrückungen. Im Normalfall sollte hier immer der Standardwert 'yes' benutzt werden.

**MKFLI4L\_DEBUG\_OPTION** Es können zum Debuggen zusätzliche Optionen an das [mkfli4l-Programm](#) (Seite 341) übergeben werden.

## 6. Anbindung von PCs im LAN

Für jeden Rechner im LAN ist einzustellen:

1. IP-Adresse (siehe [IP-Adresse](#))
2. Name des Rechners plus Wunsch-Domain-Name (siehe [Rechnername und Domain](#))
3. Standard-Gateway (siehe [Gateway](#))
4. IP-Adresse des DNS-Servers (siehe [DNS-Server](#))

### 6.1. IP-Adresse

Die IP-Adresse muss im gleichen Netz wie die IP-Adresse des fli4l-Routers (auf Ethernet-Seite) liegen, also z.B. 192.168.6.2, wenn der fli4l die Adresse 192.168.6.1 hat. Kein Rechner darf die gleiche IP-Adresse haben, weshalb man am besten (nur) die letzte Zahl ändert. Auch ist darauf zu achten, dass man hier die gleiche IP-Adresse angibt, wie man es für diesen Rechner in der Datei config/base.txt angegeben hat.

### 6.2. Rechnername und Domain

Der Name des Rechners ist dann z.B. "mein-pc", die Domain "lan.fli4l".

**Wichtig:** Die im PC eingestellte Domain muss identisch mit der gewählten Domain im fli4l-Rechner sein, wenn man den fli4l-Router als DNS-Server verwenden will. Sonst kann es im Netz erhebliche Probleme geben.

Grund: Windows-Rechner suchen regelmäßig nach Rechnern mit dem Namen ihrer Arbeitsgruppe: WORKGROUP.meine-domain.fli4l. Ist dies nicht die in fli4l eingestellte Domain (hier: meine-domain.fli4l), wird fli4l versuchen, diese Anfrage durch Weiterleiten ins Internet zu beantworten ...

Einzutragen ist die Domain in den TCP/IP Einstellungen des Rechners.

#### 6.2.1. Windows 2000

Für Windows 2000 findet man das unter:

Start ⇒

Einstellungen ⇒

Systemsteuerung ⇒

Netzwerk- und DFÜ-Verbindungen ⇒

LAN-Verbindung ⇒

Eigenschaften ⇒

Internetprotokoll (TCP/IP) ⇒

## 6. Anbindung von PCs im LAN

Eigenschaften ⇒  
Erweitert... ⇒  
DNS ⇒  
DNS-Suffix hinzufügen ⇒

“lan.fli4l” (bzw. die eingestellte domain) eingeben (ohne “”) ⇒ OK drücken.

### 6.2.2. NT 4.0

Start ⇒  
Einstellungen ⇒  
Systemsteuerung ⇒  
Netzwerk ⇒  
Protokolle ⇒  
TCP/IP ⇒  
Eigenschaften ⇒  
DNS ⇒

- Hostname eintragen (eigener Rechnername)
- Domäne eintragen (wie in config/base.txt)
- IP-Adresse vom fli4l-Router hinzufügen
- DNS-Suffix hinzufügen (Domäne hinzufügen – siehe 2 Zeilen höher)

### 6.2.3. Win95/98

Start ⇒  
Einstellungen ⇒  
Systemsteuerung ⇒  
Netzwerk ⇒  
Konfiguration ⇒  
TCP/IP (jenes, das an die Netzwerkkarte zum Router  
angebunden ist) ⇒  
Eigenschaften ⇒  
DNS-Konfiguration:  
DNS aktivieren und bei “Domäne:” dann “lan.fli4l” eingeben (ohne “”).

### 6.2.4. Windows XP

Für Windows XP findet man das unter:

Start ⇒  
Einstellungen ⇒  
Systemsteuerung ⇒  
Netzwerkverbindungen ⇒  
LAN-Verbindung ⇒  
Eigenschaften ⇒

Internetprotokoll (TCP/IP) ⇒  
Eigenschaften ⇒  
Erweitert... ⇒  
DNS ⇒  
DNS-Suffix für diese Verbindung ⇒

“lan.fli4l” (bzw. die eingestellte domain) eingeben (ohne “”) ⇒OK drücken.

### 6.2.5. Windows 7

Für Windows 7 findet man das unter:

Windows Button (ex. Start) ⇒  
Systemsteuerung ⇒  
Netzwerk und Internet ⇒  
Netzwerk- und Freigabecenter ⇒  
LAN-Verbindung ⇒  
Eigenschaften ⇒  
Internetprotokoll Version 4 (TCP/IPv4) ⇒  
Eigenschaften ⇒  
Erweitert... ⇒  
DNS ⇒  
DNS-Suffix für diese Verbindung ⇒

“lan.fli4l” (bzw. die eingestellte domain) eingeben (ohne “”) ⇒OK drücken.

### 6.2.6. Windows 8

Für Windows 8 findet man das unter:

Gleichzeitig Windows- und X-Taste drücken ⇒  
Systemsteuerung ⇒  
Netzwerk und Internet ⇒  
Netzwerk- und Freigabecenter ⇒  
Ihr Netzwerk wählen (Ethernet oder WLAN) ⇒  
Eigenschaften ⇒  
Internetprotokoll Version 4 (TCP/IPv4) ⇒  
Eigenschaften ⇒  
Erweitert... ⇒  
DNS ⇒  
DNS-Suffix für diese Verbindung ⇒

“lan.fli4l” (bzw. die eingestellte domain) eingeben (ohne “”) ⇒OK drücken.

## 6.3. Gateway

Die Angabe des Standard-Gateways ist unbedingt erforderlich, denn ohne die Angabe der richtigen IP-Adresse an dieser Stelle funktioniert nichts. Es muß hier die IP-Adresse des fli4l-

Routers (auf Ethernet-Seite) angegeben werden, also z.B. 192.168.6.4 entsprechend der IP-Adresse, die hier in der Datei config/base.txt für den fli4l-Router angegeben wurde.

Es ist falsch, den fli4l-Router als Proxy in der Windows- oder Browser- Konfiguration einzutragen – außer man setzt ein Proxy auf dem fli4l-Router ein. Im Normalfall ist fli4l kein Proxy, daher bitte *nicht* fli4l als Proxy angeben!

### 6.4. DNS-Server

Als IP-Adresse des DNS-Servers gibt man nicht die Adresse des Provider-DNS-Servers an, sondern die des fli4l-Routers (Ethernet), da dieser nun selbst Anfragen beantworten kann bzw. diese bei Unkenntnis ins Internet weiterleitet.

Mit der Konstruktion von fli4l als DNS-Server werden viele von den Windows-PCs ausgeführten Anfragen nicht ins Internet weitergeroutet, sondern werden direkt vom fli4l-Router beantwortet.

### 6.5. Verschiedenes

Die Punkte 1 bis 4 brauchen bei konfiguriertem DHCP-Server nicht eingetragen zu werden, da dann der fli4l-Router die notwendigen Daten automatisch übermittelt.

**Internetoptionen:** Bei Verbindungen muß “keine Verbindung wählen” ausgewählt sein. Bei Einstellungen für lokales Netzwerk(LAN): es darf hier NICHTS angegeben werden (es sei dann es wird OPT\_Proxy verwendet). Beides sind Standardeinstellungen, die im Normalfall nicht geändert werden müssen.

## 7. Client-/Server-Schnittstelle imon

### 7.1. imon-Server imond

imond ist ein netzwerkfähiges Server-Programm, welches bestimmte Anfragen beantwortet oder auch Kommandos zur Steuerung des Routers entgegennehmen kann.

Ausserdem steuert imond das Least-Cost-Routing. Dazu verwendet er eine Konfigurationsdatei `/etc/imond.conf`, welche beim Booten automatisch aus den `ISDN_CIRC_x_XXX`-Variablen der Datei `config/isdn.txt` und anderen über ein Shell-Script erzeugt wird.

imond läuft permanent als Daemon und horcht gleichzeitig auf TCP/IP-Port 5000 und Device `/dev/isdninfo`.

Folgende Kommandos sind über den TCP/IP-Port 5000 möglich:

Der TCP/IP-Port 5000 ist nur vom maskierten LAN aus erreichbar. Standardmäßig wird ein Zugriff von aussen über die Firewall-Konfiguration abgeblockt.

Imond unterstützt zwei Benutzerebenen: den User- und den Admin-Modus. Für beide Ebenen kann ein Passwort gesetzt werden mittels `IMOND_PASS` bzw. `IMOND_ADMIN_PASS`. Dadurch werden die imon-Clients von imond gezwungen, eine Password-Abfrage durchzuführen und anschließend das Password an imond zu übertragen. Solange dieses Password nicht übermittelt wurde, nimmt imond nur die beiden Kommandos "pass" und "quit" entgegen. Alle anderen werden mit einem Fehler zurückgewiesen.

Möchte man das weiter einschränken, z.B. den Zugriff nur von nur einem PC erlauben, muss die Firewall-Konfiguration angepasst werden.

Die Befehle

```
enable/disable/dialmode    dial/hangup    route    reboot/halt
```

können durch die Konfigurationsvariablen `IMOND_XXX` global ein- oder abgeschaltet werden (s. Kapitel "Konfiguration").

Mit einem Unix/Linux-Rechner (oder einem Windows-Rechner in der DOS-Box) kann man das Ganze leicht ausprobieren:

Nach Eingabe von

```
telnet fli4l 5000          \# oder entsprechender Name des fli4l-Routers
```

kann man direkt die oben aufgeführten Kommandos eingeben und sich die Ausgabe anschauen.

Zum Beispiel bekommt man mit "help" die Hilfe angezeigt, mit "quit" wird die Verbindung zum imond abgebaut.

#### 7.1.1. Least-Cost-Routing – Funktionsweise

imond konstruiert aus der Konfigurationsdatei `/etc/imond.conf` (welche wiederum beim Booten aus den Konfigurationsvariablen `ISDN_CIRC_x_TIMES` usw. erstellt wird), eine zeitabhängige

### Admin-Befehle

addlink ci-index	Channel zum Circuit hinzufügen (Channel-Bundling)
adjust-time seconds	Ändert die Uhrzeit des Routers um die angegebenen Sekunden
delete filename pw	Löscht die Datei auf dem Router
hup-timeout #ci-index [value]	Anzeigen bzw. Setzen des HUP-Timeout für ISDN-Circuits
removelink ci-index	Zusätzlichen Channel wieder entfernen
reset-telmond-log-file	Löschen der telmond-Protokolldatei
reset-imond-log-file	Löschen der imond-Protokolldatei
receive filename #bytes pw	Eine Datei auf den Router übertragen. Dazu quittiert imond den Befehl mit einem ACK (0x06). Danach wird die Datei in 1024er-Blöcken übertragen, die imond auch jeweils mit einem ACK bestätigt. Als letztes übermittelt imond noch ein OK.
send filename pw	Wenn das Passwort stimmt und die Datei existiert, liefert imond ein OK #bytes. Anschliessend überträgt imond die Datei in 1024er Blöcken, die jeweils mit einem ACK (0x06) bestätigt werden müssen. Als letztes liefert imond noch ein OK.
support pw	Liefert den Status/Konfiguration vom Router
sync	Synchronisiert den Cache von gemounteten Laufwerken

### Admin- oder User-Befehle

dial	Wählt den Provider an (Default-Route-Circuit)
dialmode [auto manual off]	Liefert bzw. setzt den Dialmode
disable	Hängt ein und setzt dialmode auf "off"
enable	Setzt dialmode auf "auto"
halt	Führt den Router sauber herunter
hangup [#channel-id]	Hängt ein
poweroff	Führt den Router herunter und schaltet ab
reboot	Reboot vom i4l-Router!
route [ci-index]	Setzen Default-Route auf Circuit X (0=automatisch)



## User-Befehle

channels	Ausgabe Anzahl der verfügbaren ISDN-Kanäle
charge #channel-id	Ausgabe der Online-Kosten für einen Channel
chargetime #channel-id	Online-Zeit unter Berücksichtigung des Taktes
circuit [ci-index]	Ausgabe eines Circuit-Namens
circuits	Ausgabe Anzahl der Default-Route-Circuits
cpu	Liefert die Auslastung der CPU in Prozent
date	Ausgabe Datum/Uhrzeit
device ci-index	Liefert das Device des Circuits
driverid #channel-id	Ausgabe Driver-Id für Channel X
help	Ausgabe Hilfe
inout #channel-id	Ausgabe der Richtung (incoming/outgoing)
imond-log-file	Ausgabe imond-Protokolldatei
ip #channel-id	Ausgabe der IP
is-allowed command	Ausgabe, ob Befehl konfiguriert/gültig ist Mögliche Befehle: dial dialmode route reboot  imond- log telmond-log mgetty-log
is-enabled	Ausgabe, ob dialmode auf off (0) oder auto (1)
links ci-index	Ausgabe Anzahl momentaner Channel 0, 1 oder 2, 0 heisst: Kein Channel-Bundling möglich
log-dir imond telmond mgetty	Liefert das Logverzeichnis
mgetty-log-file	Ausgabe mgetty-Protokolldatei
online-time #channel-id	Ausgabe Online-Zeit der akt. Verbindung in hh:mm:ss
pass [password]	Abfrage, ob Password nötig bzw. Password- Eingabe 1 Userpassword gesetzt 2 Adminpassword gesetzt 4 imond befindet sich im Admin-Modus
phone #channel-id	Ausgabe Telefonnummer/Name des "Gegners"
pppoe	Liefert die Anzahl der pppoe-Devices (also 0 oder 1)
quantity #channel-id	Liefert die übertragenen Datenmengen (in Byte)
quit	Beenden der Verbindung zu imond
rate #channel-id	Ausgabe Übertragungsraten (incoming/outgoing in B/sec)
status #channel-id	Ausgabe Status für Channel X
telmond-log-file	Ausgabe telmond-Protokolldatei
time #channel-id	Ausgabe Summe Online-Zeiten, Format hh:mm:ss
timetable [ci-index]	Ausgabe der Zeittabelle für LC-Routing
uptime	Ausgabe der Uptime des Routers in Sekunden
usage #channel-id	Ausgabe Art der Verbindung, mögliche Antworten: Fax, Voice, Net, Modem, Raw
version	Ausgabe der Protokoll- und Programm-Version

## 7. Client-/Server-Schnittstelle imon

Tabelle (Time-Table). Diese umfasst eine komplette Kalenderwoche im 1-Stunden-Raster (168 Stunden = 168 Bytes). Die Tabelle setzt sich jedoch lediglich aus Circuits zusammen, für die eine Default-Route definiert ist.

Mit dem imond-Kommando "timetable" kann man sich diese Tabelle anschauen.

Hier ein Beispiel:

Nehmen wir an, dass 3 Circuits definiert wurden, nämlich:

```
CIRCUIT_1_NAME='Addcom'
CIRCUIT_2_NAME='AOL'
CIRCUIT_3_NAME='Firma'
```

wobei lediglich die ersten beiden Circuits mit Default-Routen belegt sind, also die entsprechenden Variablen ISDN\_CIRC\_x\_ROUTE den Wert '0.0.0.0' haben.

Wenn die dazugehörigen Variablen ISDN\_CIRC\_x\_TIMES folgendermaßen aussehen:

```
ISDN_CIRC_1_TIMES='Mo-Fr:09-18:0.0388:N Mo-Fr:18-09:0.0248:Y
Sa-Su:00-24:0.0248:Y'

ISDN_CIRC_2_TIMES='Mo-Fr:09-18:0.019:Y Mo-Fr:18-09:0.049:N
Sa-Su:09-18:0.019:N Sa-Su:18-09:0.049:N'

ISDN_CIRC_3_TIMES='Mo-Fr:09-18:0.08:N Mo-Fr:18-09:0.03:N
Sa-Su:00-24:0.03:N'
```

dann wird daraus folgende Datei /etc/imond.conf:

#day	hour	device	defroute	phone	name	charge	ch-int
Mo-Fr	09-18	ipp0	no	010280192306	Addcom	0.0388	60
Mo-Fr	18-09	ipp0	yes	010280192306	Addcom	0.0248	60
Sa-Su	00-24	ipp0	yes	010280192306	Addcom	0.0248	60
Mo-Fr	09-18	ipp1	yes	019160	AOL 0.019	180	
Mo-Fr	18-09	ipp1	no	019160	AOL 0.049	180	
Sa-Su	09-18	ipp1	no	019160	AOL 0.019	180	
Sa-Su	18-09	ipp1	no	019160	AOL 0.049	180	
Mo-Fr	09-18	isd2	no	0221xxxxxxx	Firma	0.08	90
Mo-Fr	18-09	isd2	no	0221xxxxxxx	Firma	0.03	90
Sa-Su	00-24	isd2	no	0221xxxxxxx	Firma	0.03	90

imond erstellt dann im Speicher folgende Time-Table – hier die Ausgabe über das imond-Kommando "timetable":

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Su	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
Mo	2	2	2	2	2	2	2	2	2	4	4	4	4	4	4	4	4	4	2	2	2	2	2	2
Tu	2	2	2	2	2	2	2	2	2	4	4	4	4	4	4	4	4	4	2	2	2	2	2	2
We	2	2	2	2	2	2	2	2	2	4	4	4	4	4	4	4	4	4	2	2	2	2	2	2
Th	2	2	2	2	2	2	2	2	2	4	4	4	4	4	4	4	4	4	2	2	2	2	2	2
Fr	2	2	2	2	2	2	2	2	2	4	4	4	4	4	4	4	4	4	2	2	2	2	2	2
Sa	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3

No.	Name	DefRoute	Device	Ch/Min	ChInt
1	Addcom	0.0.0.0	ipp0	0.0388	60
2	AOL	0.0.0.0	ipp1	0.019	180
3	Firma	0.0.0.0	isd2	0.08	90

## 7. Client-/Server-Schnittstelle imon

1	Addcom		no	ipp0	0.0388	60
2	Addcom		yes	ipp0	0.0248	60
3	Addcom		yes	ipp0	0.0248	60
4	AOL	yes	ipp1	0.0190	180	
5	AOL	no	ipp1	0.0490	180	
6	AOL	no	ipp1	0.0190	180	
7	AOL	no	ipp1	0.0490	180	
8	Firma		no	isd2	0.0800	90
9	Firma		no	isd2	0.0300	90
10	Firma		no	isd2	0.0300	90

Für den Circuit 1 (Addcom) sind also drei Zeitbereiche (1-3) eingetragen, für Circuit 2 (AOL) vier Zeitbereiche (4-7) und für den letzten drei Zeitbereiche (8-10).

In der Time-Table werden jeweils die Indices ausgegeben, welche für die jeweilige Stunde gültig sind. Hier tauchen lediglich die Indices 2-4 auf, da alle anderen keine LC-Default-Routen sind.

Sieht man in der Tabelle irgendwo Nullen, gibt es Lücken in den ISDN\_CIRC\_X\_TIMES-Werten. Dann existiert zu diesen Zeiten keine Default-Route, Internet-Zugang abgeknipst!

Beim Programmstart ermittelt imond zunächst den Wochentag und die aktuelle Stunde. Anschließend wird dann über die Time-Table der Index ermittelt und damit dann auch der entsprechende Circuit. Auf diesen wird dann die Default-Route gesetzt.

Bei Zustandsänderungen der Channels, z.B. Wechsel von online nach offline – jedoch spätestens nach 1 Minute – geht das Spiel von neuem los: Zeit ermitteln, Lookup in Tabelle, Default-Route-Circuit ermitteln.

Ändert sich der aktuell verwendete Circuit, z.B. montags um 18:00 Uhr, wird die alte Default-Route gelöscht, eine vielleicht bestehende Verbindung beendet (sorry...) und anschließend die Default-Route auf den neuen Circuit gesetzt. Dies kann von imond bis zu 60 Sekunden später bemerkt werden, also wird spätestens um 18:00:59 umgeschaltet.

Bei Circuits, die keine Default-Route belegen, ändert sich überhaupt nichts. Hier wird der Inhalt von ISDN\_CIRC\_x\_TIMES lediglich zur Berechnung der Telefonkosten verwendet. Diese können dann relevant sein, wenn man über den Client imonc das LC-Routing temporär ausschaltet und einen Circuit manuell wählt.

Man kann sich jedoch auch die Tabellen für andere Zeitbereich-Indices (im Beispiel von 1 bis 10) anschauen, auch die der "Non-LC-Default-Route-Circuits".

Kommando:

```
timetable index
```

Beispiel:

```
telnet fli41 5000
timetable 5
quit
```

Die Ausgabe sieht dann so aus:

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Su	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Mo	5	5	5	5	5	5	5	5	5	0	0	0	0	0	0	0	0	0	5	5	5	5	5	5

Tu	5	5	5	5	5	5	5	5	5	0	0	0	0	0	0	0	0	5	5	5	5	5	5
We	5	5	5	5	5	5	5	5	5	0	0	0	0	0	0	0	0	5	5	5	5	5	5
Th	5	5	5	5	5	5	5	5	5	0	0	0	0	0	0	0	0	5	5	5	5	5	5
Fr	5	5	5	5	5	5	5	5	5	0	0	0	0	0	0	0	0	5	5	5	5	5	5
Sa	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

No.	Name	DefRoute	Device	Ch/Min	ChInt
5	AOL	no	ipp1	0.0490	180

Alles klar?

Mit dem imond-Kommando "route" kann das LC-Routing ein- und ausgeschaltet werden. Bei Angabe eines positiven Circuit-Indices (1...N) wird die Default-Route auf den angegebenen Circuit gelegt. Ist der Index 0, wird das LC-Routing wieder aktiviert und der Circuit automatisch ausgewählt.

### 7.1.2. Zur Berechnung der Onlinekosten

Das ganze Modell zur Berechnung der Onlinekosten funktioniert nur korrekt, wenn der Zeittakt für einen Circuit (Variable `ISDN_CIRC_x_CHARGEINT`) über die ganze Woche konstant ist. Dies ist im Normalfall bei Internet-Providern die Regel. Wählt man sich jedoch über die Telekom (ich meine nicht T-Online!) z.B. in sein Firmennetz ein, gilt das als ganz normales Telefongespräch. Und da wechselt ab 18:00 der Takt von 90 Sekunden auf 4 Minuten (Stand Juni 00). Deshalb ist die Definition von

```
ISDN_CIRC_3_CHARGEINT='90'
ISDN_CIRC_3_TIMES='Mo-Fr:09-18:0.08:N Mo-Fr:18-09:0.03:N Sa-Su:00-24:0.03:N'
```

eigentlich nicht ganz korrekt. Es sind zwar abends umgerechnet auf die Minute 3 Pfennig (4 Minuten kosten 12 Telekom-Pfennige), jedoch ist der Takt falsch. Deshalb können bei der Kostenanzeige Differenzen zu den tatsächlichen Zahlen auftreten.

Hier ist ein Tipp, wie verschieden lange Taktzeiten dennoch richtig berücksichtigt werden können (auch wichtig für `ISDN_CIRC_x_CHARGEINT`): Man definiert einfach 2 Circuits, einen für tagsüber mit `ISDN_CIRC_1_CHARGEINT='90'` und den anderen mit `ISDN_CIRC_2_CHARGEINT='240'`. Natürlich muss man dann auch noch `ISDN_CIRC_x_TIMES` entsprechend wählen, damit tagsüber Circuit 1 und abends Circuit 2 verwendet wird.

Wie gesagt: Bei Nutzung von Verbindungen zu Internet-Providern gibt es das Problem nicht, weil dort der Zeittakt immer konstant ist und lediglich die Kosten pro Minute wechseln (oder gibt es sowas doch??? Ich traue T-\* alles zu :-).

## 7.2. Windows-Client imonc.exe

### 7.2.1. Einleitung

Das Gespann imond auf dem Router und imonc auf dem Client beherrschen zwei Benutzermodi: den User- und den Adminmodus. Im Adminmodus sind alle Steuerelemente aktiviert. Im Usermodus steuern die Variablen `IMOND_ENABLE` (Seite 86), `IMOND_DIAL` (Seite 85), `IMOND_ROUTE` (Seite 85) und `IMOND_REBOOT` (Seite 85) ob die jeweiligen Funktionen im Usermodus zur Verfügung stehen. Sind alle diese Variablen auf 'no' gesetzt, bedeutet dies für die Überblick-Seite,

dass alle Buttons bis auf den Exit- und den Admin-Mode-Button deaktiviert sind. Die Entscheidung, ob der User- oder Admin-Modus benutzt wird, wird anhand des übermittelten Passwortes getroffen. Über den Button Admin-Mode, der sich in der Statusleiste befindet, kann jederzeit unter Eingabe des Admin-Passwortes vom User- zum Admin-Modus gewechselt werden. Um wieder zurück zu wechseln, muss imonc beendet und neu gestartet werden.

Sobald imonc gestartet ist, wird ein zusätzliches Tray-Icon angezeigt, welches den Verbindungsstatus der vorhandenen Kanäle anzeigt.

Die Farben bedeuten:

**Rot** : Offline

**Gelb** : Es wird gerade eine Verbindung aufgebaut

**Hellgrün** : Online und Traffic auf dem Kanal

**Dunkelgrün** : Online und so gut wie kein Traffic auf dem Kanal

Ein etwas vom Windows-Standard abweichendes Verhalten zeigt imonc, wenn der Minimieren-Button in der Titelleiste angeklickt wird. Daraufhin minimiert sich imonc in den Systemtray und es bleibt nur noch das Tray-Icon neben der Uhr übrig. Ein Doppelklick mit der linken Maustaste auf das Tray-Symbol holt das imonc-Fenster wieder in den Vordergrund. Mit der rechten Maustaste besteht auch die Möglichkeit über das Kontextmenü, die wichtigsten imonc-Kommandos direkt auszuwählen, ohne imonc wieder auf den Bildschirm zu holen.

Viele Eigenschaften (darunter auch alle Spaltenbreiten der StringGrids) speichert imonc in der Registry, damit imonc so an die eigenen Bedürfnisse angepasst werden kann. Imonc speichert die Informationen in dem Registry-Schlüssel HKCU\Software\fli4l.

Bestehen trotz sorgfältigen Lesens der Dokumentation noch Probleme in Bezug auf imonc oder auch des Routers selber, die man z.B. in der Newsgroup posten möchte, ist es sinnvoll, auf der Über-Seite des imonc den Punkt SystemInfo auszuwählen und dort den Punkt Support Infos. Daraufhin wird das Router-Passwort abgefragt (nicht das imonc-Passwort!). Imonc erstellt dann eine Datei fli4lsup.txt, welche alle wichtigen Informationen bezüglich des Routers und imonc beinhaltet. Diese Datei kann auf explizite Nachfrage in die Newsgroup gepostet werden, so dass deutlich bessere Chancen auf rasche Hilfe bestehen.

Nähere Details betreffend der Entwicklung des Windows-Clients imonc findet man auf der Homepage vom Windows ImonC-Seiten <http://www.imonc.de/>. Hier kann man sehen, welche neuen Features und Bug-Fixes in der nächsten Version von imonc enthalten sein werden. Ausserdem gibt es dort den neusten imonc, wenn dieser nicht schon in der fli4l-Distribution enthalten ist.

### 7.2.2. Startparameter

ImonC benötigt den Namen oder die IP-Adresse des fli4l-Routers. Standardmäßig versucht das Programm, eine Verbindung mit dem Rechner "fli4l" herzustellen. Wenn dieser im DNS korrekt eingetragen ist, sollte es also direkt funktionieren. Ansonsten kann man in der Verknüpfung folgende Parameter übergeben:

- /Server:IP oder Hostname des Routers (Kurzform: /S:IP oder Hostname)
- /Password:Passwort (Kurzform: /P:Password)

- `/log` Die Logging-Option zum Protokollieren der Kommunikation zwischen imonc und imond. Ist diese Option eingeschaltet, wird beim Beenden von imonc eine Datei imonc.log geschrieben. Diese Datei beinhaltet die gesamte Kommunikation zwischen Router und Client und wird darum sehr groß. Deshalb sollte dieser Startparameter nur gesetzt werden, wenn Probleme bestehen.
- `/iport:Portnummer` Die Portnummer auf die imond lauscht. Default: 5000
- `/tport:Portnummer` Port auf dem telmond lauscht. Default: 5001
- `/rc:"Command"` Das hier angegebene Kommando wird ohne weitere Überprüfung an den Router übertragen und anschliessend imonc beendet. Sollen mehrere Kommandos gleichzeitig ausgeführt werden, müssen diese durch Semikolons getrennt werden. Damit es funktioniert, muss ein gesetztes imond-Passwort mit übergeben werden, da keine Abfrage des Passwortes erfolgt. Die möglichen Kommandos sind beim imond dokumentiert, siehe Kapitel 8.1. Zusätzlich zu den dort aufgeführten Befehlen gibt es noch den Befehl `timesync`. Dieser bewirkt, dass die Uhrzeit des Clients mit der des Routers synchronisiert wird. Der Befehl `dialtimesync` wird nicht mehr unterstützt da er sich als „dial; timesync“ schreiben lässt.
- `/d:"fli4l-Directory"` Hiermit kann das fli4l-Directory per Startparameter übergeben werden. Interessant wenn man mit mehreren fli4l-Versionen herumspielt
- `/wait` Wenn der Hostname nicht aufgelöst werden kann, beendet sich imonc nicht mehr – erneuter Verbindungsaufbau durch Doppelclick auf das TrayIcon
- `/nostartcheck` Dieser schaltet die Überprüfung ab, ob imonc bereits läuft. Nur sinnvoll, wenn mehrere, unterschiedliche fli4l-Router in einem Netz überwacht werden sollen. Bei weiteren Instanzen werden die eingebauten Syslog- und E-Mail-Funktionalitäten deaktiviert.

Usage (einzutragen in der Verknüpfung):

```
X:\...imonc.exe [/Server:Host] [/Password:Passwort] [/iport:Portnummer]
                [/log] [/tport:Portnummer] [/rc:"Command"]
```

Beispiel mit IP-Adresse:

```
C:\wintools\imonc /Server:192.168.6.4
```

oder mit Namen und Passwort:

```
C:\wintools\imonc /S:fli4l /P:geheim
```

oder mit Namen, Passwort und Routerkommando:

```
C:\wintools\imonc /S:fli4l /P:geheim /rc:"dialmode manual"
```

### 7.2.3. Seite Überblick

Der Windows-Client fragt einige imond-Informationen über die bestehenden Verbindungen ab und bereitet sie im Anzeigefenster auf. Neben generellen Statusinformationen wie Uptime des Router oder auch der Uhrzeit sowohl lokal wie auch vom Router selber, werden für jede bestehende Verbindung die folgenden Informationen angezeigt:

Status	Verbindungsaufbau/Online/Offline
Name	Telefonnummer des Gegners oder Circuit-Name
Richtung	Zeigt an, ob es sich um eine eingehende oder ausgehende Verbindung handelt
IP	Die IP, die man zugewiesen bekommen hat
IBytes	Empfangene Bytes
OBytes	Gesendete Bytes
Online-Zeit	Aktuelle Online-Zeit
Zeit	Summe aller Online-Zeiten
KZeit	Summe Online-Zeiten unter Berücksichtigung des Zeittaktes
Kosten	Berechnete Kosten

Die Daten werden standardmäßig alle 2 Sekunden aktualisiert. Im Kontextmenü dieser Übersicht besteht die Möglichkeit für jeden vorhandenen Kanal, mit dem der Router gerade online ist, sowohl die zugewiesene IP in die Zwischenablage zu kopieren, als auch den Kanal gezielt auflegen zu können. Letzteres ist für den Fall interessant, dass mehrere unterschiedliche Verbindungen bestehen, z.B. eine um im Internet zu surfen und eine andere zur Firma, und gezielt eine dieser Verbindungen getrennt werden soll.

Ist zusätzlich auf dem fli4l-Router der telmond-Prozess aktiv, kann imonc zusätzlich Informationen über eingehende Telefonanrufe (nämlich anrufende und angerufene MSN) anzeigen. Der letzte eingegangene Telefonanruf wird oberhalb der Buttons angezeigt. Ein Protokoll der eingegangenen Telefonanrufe erhält man durch Anzeige der Seite Anrufe.

Mit den sechs Buttons im imonc können folgende Kommandos angewählt werden:

Button	Beschriftung	Funktion
1	Verbinden/Trennen	Wählen/Einhängen
2	Add link/Rem link	Kanäle bündeln: ja/nein – dieses Feature steht nur im Admin-Mode zur Verfügung
3	Reboot	fli4l neu booten!
4	PowerOff	fli4l sauber runterfahren und anschliessend ausschalten
5	Halt	fli4l sauber runterfahren, um ihn anschliessend sicher ausschalten zu können
6	Beenden	Client beenden

Die ersten fünf Kommandos können in der Konfigurationsdatei des fli4l-Routers config/base.txt für den User-Modus einzeln ein- und ausgeschaltet werden. Im Admin-Modus sind immer alle aktiviert. Die Auswahl Dialmode steuert das Wahlverhalten des Routers:

Auto	Der Router baut automatisch eine Verbindung auf dem entsprechenden Circuit auf, wenn eine Anfrage aus dem lokalen Netz eintrifft.
Manuell	Der Benutzer muss selber die Verbindung aufbauen.
Aus	Es ist weder manuell noch automatisch möglich, eine Verbindung aufzubauen. Der Dial-Button ist dann deaktiviert.

Bleibt noch anzumerken, dass fli4l standardmäßig selbständig rauswählt, wenn man mit seinem Rechner in's Internet will. Man muss also eigentlich nie den Verbinden-Button drücken ...

Es besteht auch die Möglichkeit, den Default-Route-Circuit manuell zu wechseln, also das automatische LCR-Routing ein- und auszuschalten. Dafür ist in der Windows-Version von imonc die Auswahlliste "Default Route" vorgesehen. Ausserdem kann man die Hangup-TimeOut-Zeit jetzt auch über imonc direkt konfigurieren. Dazu dient der Button Config neben der Default Route. Dort werden alle konfigurierten Circuits des Routers angezeigt. Der Wert in der Spalte Hup-timeout kann für ISDN-Circuits direkt im StringGrid editiert werden (funktioniert bis dato noch nicht für DSL).

Einen Überblick über das LCR-Routing findet man auf der Seite Admin/TimeTable. Dort sieht man, welchen Circuit imond zu welcher Zeit automatisch auswählt.

#### 7.2.4. Config-Dialog

Der Konfigurationsbereich ist über den Button Config in der Statuszeile erreichbar. Das aufgehende Fenster ist dann in die folgenden Bereiche unterteilt:

- Der Bereich Allgemein:
  - Aktualisierungsintervall: Hier wird eingestellt, wie oft die Seite Überblick aktualisiert werden soll.
  - Zeit beim Programmstart synchronisieren: Übernimmt beim Starten des Client die Zeit und das Datum des Routers als lokale Zeit. Diese Funktion kann auch manuell mit dem Button Synchronisieren auf der Überblicks-Seite aufgerufen werden.
  - Minimiert starten: Startet das Programm direkt minimiert, man sieht nur das Icon neben der Uhr.
  - Zusammen mit Windows starten: Hier kann man angeben, ob der Client direkt beim Starten von Windows mit gestartet werden soll. In dem Feld Parameter kann man die nötigen Start-Parameter angeben.
  - News von fli4l.de abholen: Sollen die News, die auf der fli4l-Homepage in der News-Sektion angezeigt werden, auch vom imonc geholt und angezeigt werden? Die Schlagzeilen werden dann in der Statusbar angezeigt. Ausserdem wird dann eine neue Seite News angezeigt, in der die kompletten Meldungen angezeigt werden.
  - Logdatei für Verbindungen: Den Dateinamen, den man hier angeben kann, wird dazu benutzt, die Verbindungs-Liste unter diesem Namen lokal auf dem Rechner abzuspeichern.
  - TimeOut für Router zum antworten: Wie lange soll auf eine Antwort der Routers gewartet werden, bevor angenommen wird, dass die Verbindung nicht mehr besteht.
  - Sprache: Hier kann die Sprache des imoncs ausgewählt werden.



- Router Befehle bestätigen: Ist dieses Feature aktiviert, müssen alle Router-beeinflussenden Kommandos, wie zum Beispiel Reboot, Hangup . . . generell bestätigt werden.
  - Auflegen auch bei Traffic: Soll kein Hinweis erfolgen, wenn die Verbindung beendet wird und noch Traffic auf der Leitung ist.
  - Automatisch Verbindung zum Router aufbauen: Soll, wenn die Verbindung zum Router unterbrochen wird (z.B. durch einen Neustart des Routers), automatisch probiert werden, die Verbindung wieder herzustellen.
  - Fenster in System Tray minimieren: Soll imonc beim Klicken auf den Beenden-Button in der Titelleiste sich in den System-Tray neben der Uhr minimieren anstatt zu beenden.
- Der Unterbereich Proxy: Hier kann ein Proxy für die http-Anfragen des imoncs definiert werden. Dieser wird dann zur Zeit für das Holen der News benutzt.
    - Proxy-Unterstützung für Http-Anfragen aktivieren: Soll ein Proxy benutzt werden
      - \* Adresse: Die Adresse des Proxy-Servers
      - \* Port: Die Portnummer des Proxy-Server (default: 8080)
  - Der Unterbereich TrayIcon: Hier können die Farben des TrayIcons neben der Uhr an die eigene Bedürfnisse angepasst werden. Weiterhin kann ausgewählt werden, dass der aktuelle Dialmode als farblicher Hintergrund des TrayIcons dargestellt wird.
  - Der Bereich Anrufe: Die Position des Call Notification-Fensters wird in der Registry gespeichert, so dass man sich das Fenster an die Position schieben kann, wo man es haben möchte. Es erscheint anschliessend immer wieder an dieser Stelle.
    - Aktualisierung: Hier kann ausgewählt werden, wie imonc über neue Anrufe informiert wird. Es gibt drei verschiedene Möglichkeiten. Diese erste besteht darin, regelmäßig den telmond-Dienst auf dem Router abzufragen. Eine weitere Möglichkeit besteht in der Auswertung der Syslog-Meldungen. Diese Variante ist der ersten vorzuziehen – dazu muss natürlich der Syslog-Client des imonc aktiviert sein. Wird imonc mit einem routenden eisfair eingesetzt, bietet sich noch die Möglichkeit das Capi2Text-Paket zur Anrufsignalisierung zu benutzen.
    - Führende Null wegen Telefonanlage löschen: Telefonanlage setzen manchmal eine zusätzliche Null vor die Rufnummer des Anrufer. Diese kann mit dieser Option unterdrückt werden.
    - Eigene Vorwahl: Hier kann die eigene Vorwahl hinterlegt werden. Wann dann ein Anruf mit gleichen Vorwahl eintrifft, wird die gesendete Vorwahl ausgeblendet.
    - Telefonbuch: Hier kann die Datei angegeben werden, in der das lokale Telefonbuch zur Auflösung von Telefonnummer gespeichert wird. Existiert die Datei nicht, wird sie vom Programm angelegt.
    - Logdatei: Der Dateinamen, den man hier angeben kann, wird dazu benutzt, die Calls-Liste unter diesem Namen lokal auf dem Rechner zu speichern. Dieser Menüpunkt ist nur sichtbar, wenn die Config-Variable TELMOND\_LOG auf 'yes' gesetzt ist, dieses gilt auch für die eigentliche Anruf-Liste.

- Externes Suchprogramm benutzen: In diesem Bereich kann ein Programm angegeben werden, dass aufgerufen wird, wenn eine Telefonnummer mittels des lokalen Telefonbuches nicht aufgelöst werden kann. Nähere Infos sollten den entsprechenden Programmen beiliegen. Bis jetzt gibt es eine Anbindung an die Telefonbuch-CD KlickTel sowie von Marcel Wappler eine Anbindung an die Palm-Datenbank.
- Der Unterbereich Call Notification: Hier kann das bestimmt werden, ob ein Hinweis auf eingehende Telefonanrufe angezeigt werden soll und wie dieser sich optisch präsentiert.
  - Call Notification aktivieren: Bestimmt, ob Anrufe signalisiert werden sollen.
  - Call Notification anzeigen: Soll bei eingehenden Anrufen ein Hinweisfenster mit den Infos: angerufene MSN, Rufnummer des Anrufers und Datum/Uhrzeit erscheinen? Dafür ist es nötig, dass in der Datei config/isdn.txt die Variable OPT\_TELMOND auf ‘yes’ gesetzt wird.
    - \* Unterdrücken, wenn keine Nummer übertragen wurde: Soll Die Call Notification nicht angezeigt werden, wenn keine Rufnummer übertragen wurde.
    - \* Anzeigendauer: Diese Angabe beeinflusst die Dauer, wie lange das Call Notification-Fenster geöffnet bleiben soll. Die Angabe von “0” an dieser Stelle bewirkt, dass das Fenster nicht automatisch geschlossen wird.
    - \* Fontsize: Hiermit wird die Schriftgröße bestimmt. Dieses hat einen Einfluss auf die Größe des Fenster, da die notwendige Größe des Fenster anhand der tatsächlichen Größe der Mitteilung berechnet wird.
    - \* Farbe: Hiermit kann die Schriftfarbe ausgewählt werden. Ich selber benutzte die Farbe rot, damit ich es auch direkt wahrnehme.
- Der Unterbereich Phonebook: Die Seite Phonebook beinhaltet das Telefonbuch, welches zur Rufnummerrauflösung der anrufenden Nummer als auch der eigenen MSN benutzt wird. Die Seite wird auch angezeigt, wenn die Konfigurationsvariable TELMOND\_LOG auf ‘no’ gesetzt ist, da die Rufnummerrauflösung auch für die Anzeige des letzten Anrufes auf der Summary-Seite benutzt wird. Alternativ kann statt dem Telefonbuch auf dem Router auch eine lokale Datei ausgewählt werden.

Der Aufbau der Eintrag sieht wie folgt aus:

```
# Format:
# Telefonnummer=anzuzeigender Name[, Wavefilename]
# 0241123456789=Testuser
00=unbekannt
508402=Fax
0241606*=Elsa AG Aachen
```

Dabei sind die ersten drei Zeilen Kommentare. Die vierte Zeile bewirkt, dass, wenn keine Rufnummer übermittelt wird, “unbekannt” angezeigt wird. In der fünften Zeile wird der MSN 508402 der Name “Fax” zugeordnet. Ansonsten ist das Format immer Telefonnummer=Name, der stattdessen angezeigt werden soll. In der sechsten Zeile ist noch die Möglichkeit demonstriert, eine Sammelrufnummer zu definieren. Damit wird erreicht, dass für alle Nebenstellen von 0241606 der Name angezeigt wird. Zu beachten hierbei ist, dass der erste Eintrag im Telefonbuch, welcher auf den Anruf passt, genommen

wird. Optional kann auch noch ein Wave-Datei angegeben werden, die abgespielt wird, wenn ein Telefonanruf von dieser Rufnummer eingeht.

Ab der Version 1.5.2 besteht jetzt auch die Möglichkeit auf der Seite Names das lokale Telefonbuch mit dem auf dem Router abgespeicherten (in /etc/phonebook) zu synchronisieren und umgekehrt. Dabei werden nicht nur einfach die Dateien ersetzt, sondern es werden die noch fehlende Einträge hinzugefügt. Gibt es eine Telefonnummer in beiden Telefonbüchern mit unterschiedlichen Namen, wird nachgefragt, welcher Eintrag genommen werden soll. Für die Synchronisierung des Telefonbuches auf dem Router ist noch anzumerken, dass dieses nur in der Ramdisk verändert wird, d.h. dass nach einem Reboot sämtliche Änderungen verloren gehen.

- Der Bereich Sound: Die Wave-Dateien, die hier angegeben werden, werden abgespielt, wenn das jeweilige Ereignis eingetreten ist.
  - E-Mail: Wenn der E-Mail-Checker auf einem angegebenen POP3-Server neue E-Mails vorfindet, wird die angegebene Wave-Datei abgespielt.
  - E-Mail-Error: Wenn ein Fehler beim Abrufen der E-Mails auftritt, wird diese Wave-Datei abgespielt.
  - Verbindung verloren: Wenn die Verbindung zum Router nicht mehr vorhanden ist (z.B. wenn der Router von einem anderen Client gerade neu gebootet wird), wird diese Wave-Datei abgespielt. Wenn die Option “Automatic Reconnect to router” nicht aktiviert ist, erscheint ausserdem eine MessageBox, die nachfragt, ob versucht werden soll, eine neue Verbindung zum Router aufzubauen.
  - Verbindungsmeldung: Wenn der Router eine Verbindung zum Internet aufgebaut hat, wird diese Wave-Datei abgespielt.
  - Verbindungsabbau: Wenn der Router die Verbindung zum Internet wieder abgebaut hat, wird diese Wave-Datei abgespielt.
  - Anrufmeldung: Wenn die Call Notification aktiviert ist und ein neuer Anruf eingeht, wird die angegebene Wave-Datei abgespielt.
  - Fax Notification: Die hier angegebene Wave-Datei wird nach dem Empfang neuer Faxe abgespielt.
- Der Bereich E-Mails
  - Accounts: Dieser Bereich dient dazu, die vorhandenen POP3-Accounts zu konfigurieren.
  - E-Mail-Check aktivieren: Soll der E-Mail-Checker automatisch nach neuen E-Mails suchen
    - \* Check jede x Min: Hiermit wird angegeben, wie oft der E-Mail-Checker automatisch nach neuen E-Mails suchen soll. Achtung: ein zu kurzes Intervall kann dazu führen, dass der Router komplett online bleibt! Dies ist der Fall, wenn das Intervall kleiner ist als der Hangup-Timeout des verwendeten Circuits.
    - \* TimeOut x Sec: Wie lange soll auf einen POP3-Server gewartet werden, bis er antwortet. Der Wert “0” bedeutet, dass kein TimeOut gesetzt wird.

- \* Auch wenn Router offline: Hiermit wird erreicht, dass der Router sich selbstständig einwählt, um nach E-Mails zu sehen. Nachdem alle POP3-Konten nach E-Mails überprüft worden sind, wird die Verbindung wieder getrennt. Um dieses Feature nutzen zu können, muss Dialmode auf 'auto' stehen. Achtung: Dadurch entstehen zusätzliche Kosten, wenn nicht gerade eine Flatrate benutzt wird!
  - \* Zu benutzender Circuit: Hiermit wird angegeben, welcher Circuit zur Einwahl beim E-Mail-Checken benutzt werden soll.
  - \* Anschliessend online bleiben: Soll direkt nach dem E-Mail-Check direkt die Verbindung getrennt werden oder eine Verbindungstrennung durch das Hangup-timeout realisiert werden.
  - \* E-Mail-Header laden: Sollen auch die E-Mail-Header geladen oder nur die Anzahl der vorhandenen E-Mails abgefragt werden? Das Laden der E-Mail-Header ist Voraussetzung, wenn man E-Mails direkt auf dem Server löschen möchte.
  - \* Notify only new E-Mails: Sollen nur neue E-Mails akustisch und mit dem Tray-Icon gemeldet werden
  - \* E-Mail-Client starten: Soll der angegebene E-Mail-Client automatisch gestartet werden, wenn neue E-Mails vorhanden sind.
  - \* E-Mail-Client: Hier wird der zu startende E-Mail-Client angegeben.
  - \* Param: Hier kann man zusätzliche Parameter angeben, die beim Start des E-Mail-Clients übergeben werden sollen. Wenn Outlook als E-Mail-Client benutzt wird (nicht Outlook Express), sollte /recyle als Parameter eingetragen werden, damit eine bereits geöffnete Instanz von Outlook beim Eintreffen von neuen E-Mails benutzt wird.
- Der Bereich Admin
    - root-Passwort: Hier sollte das Router-Passwort (in config/base.txt unter **PASSWORD** eingetragen) eingetragen werden, damit z.B. das Portforwarding lokal bearbeitet und wieder auf dem Router hinterlegt werden kann.
    - Dateien auf dem Router, die angezeigt werden sollen: Alle hier angegebenen Dateien, die sich auf dem Router befinden, können einfach per Maus-Click auf der Seite Admin/Dateien angezeigt werden. Somit kann man sich auf einfache Weise die Logfiles des Routers direkt im imonc anzeigen lassen.
    - Konfigdateien bearbeiten: Hier kann ausgewählt werden, ob die Konfigdateien alle im Editor geöffnet werden sollen (dies kann, wenn TXT-Dateien noch mit einem einfachen Editor verknüpft sind, dazu führen, dass sehr viele Instanzen des Editors geöffnet werden). Alternativ kann auch einfach nur das Verzeichnis geöffnet werden, so dass die Möglichkeit besteht, nur die Dateien auszuwählen, die bearbeitet werden sollen.
    - DynEisfaiLog: Wenn ein Account bei DynEisfair vorhanden ist, kann man hier seine Zugangsdaten eintragen und sich dann ein Log der Aktualisierung des Dienstes auf der Seite Admin/DynEisfairLog anschauen.
  - Der Bereich LaunchList dient dazu, die Launchliste zu konfigurieren. Diese wird nach einem erfolgreichen Connect ausgeführt, wenn die Option "Activate Launchlist" aktiviert ist.

- Programme: Alle hier eingetragenen Programme werden automatisch gestartet, sobald der Router eine Verbindung aufgebaut hat und die Launchliste aktiviert ist.
- LaunchList aktivieren: Soll die Launchliste beim erfolgreichen Verbindungsaufbau ausgeführt werden?
- Der Bereich Traffic dient dazu, dass TrafficInfo-Fenster den eigenen Bedürfnissen anzupassen. Von einem User habe ich den Hinweis bekommen, dass es mit älteren DirectX-Versionen offenbar Darstellungsfehler gibt.
  - Separates Traffic-Info-Fenster anzeigen: Soll eine grafische Kanalauslastung in einem separaten Fenster angezeigt werden? In dem Kontextmenü des Fensters kann man festlegen, ob das Fenster das Attribut StayOnTop bekommen soll. Dieses bewirkt, dass sich das Fenster immer über allen anderen Fenstern plaziert. Auch dieser Wert wird in der Registry abgespeichert und steht somit auch nach einem erneuten Programmstart wieder zur Verfügung.
  - Titelleiste anzeigen: Soll die Titelleiste des Traffic-Info-Fensters angezeigt werden? In der Titelzeile wird angezeigt, mit welchem Circuit der Router gerade online ist.
    - \* CPU-Auslastung in Titelleiste: Soll auch die CPU-Auslastung in der Titelzeile angezeigt werden?
    - \* Online-Zeit in Titelleiste: Soll die Onlinezeit des Kanals auch in der Titelzeile angezeigt werden?
  - Semi-transparentes Fenster: Soll das Fenster transparent dargestellt werden? Diese Funktion steht nur unter Windows 2000 und Windows XP zur Verfügung.
  - Farben: Hier werden die Farben für das TrafficInfo-Fenster definiert. Zu Berücksichtigen ist dabei, dass der DSL-Kanal und der erste ISDN-Kanal die selben Farbwerte zugewiesen bekommen.
  - Limits: Hier können die max. Übertragungswerte für DSL eingestellt werden – Upload und Download.
- Der Bereich Syslog dient dazu, die Anzeige der Syslog-Meldungen zu konfigurieren.
  - Syslog-Client aktivieren: Sollen Syslog-Meldungen im imonc angezeigt werden? Diese Option sollte ausgeschaltet sein, wenn ein externer Syslog-Client, wie zum Beispiel Kiwi's Syslog Client, benutzt wird.
  - Alle Meldungen ab Stufe anzeigen: Ab welcher Prioritätsstufe sollen die Syslog-Meldungen angezeigt werden? Es ist sinnvoll am Anfang mit der Stufe Debug anzufangen, um damit festzustellen, welche Meldungen einen interessieren. Anschliessend kann hier dann die entsprechende Stufe eingetragen werden.
  - Syslog-Meldungen in einer Datei speichern: Sollen die angezeigten Syslog-Meldungen in einer Datei gespeichert werden? In der Groupbox können dann die Meldungen ausgewählt werden, die in der Datei geloggt werden sollen. Für den Dateinamen sind folgende Platzhalter eingefügt worden:
    - %y** – wird durch das aktuelle Jahr ersetzt
    - %m** – wird durch den aktuellen Monat ersetzt
    - %d** – wird durch den aktuellen Tag ersetzt

- Portnamen anzeigen: Sollen statt den Portnummern deren Bedeutungen angezeigt werden?
- Firewall-Meldungen auch im User-Modus anzeigen: Hiermit wird festgelegt, dass Firewall-Meldungen auch im User-Modus angezeigt werden sollen.
- Der Bereich Fax dient dazu, die Faxanzeige vom imonc zu konfigurieren. Damit dieser Punkt angezeigt wird, muss mgetty bzw. faxrcv auf dem Router installiert sein (zu finden als OPT-Pakete auf der fli4l-Homepage).
  - Logdatei für Faxe: Den Dateinamen, den man hier angeben kann, wird dazu benutzt, die Fax-Liste unter diesem Namen lokal auf dem Rechner abzuspeichern.
  - Lokales Verzeichnis: Um die Faxe anzeigen zu können, müssen sie lokal gespeichert werden. Dieses kann hier eingestellt werden.
  - Aktualisierung: Es gibt zwei verschiedene Möglichkeiten, wie imonc mitbekommt, dass ein neues Fax eingegangen ist. Entweder wertet imonc die entsprechenden Syslogmeldungen aus (dazu muss natürlich der Syslog-Client im imonc aktiviert sein) oder er schaut regelmäßig selber in der Logdatei nach. Die erste Variante ist zu bevorzugen. Falls die zweite Variante genutzt wird, kann man noch angeben, wie oft die Faxübersichtsseite aktualisiert werden soll. Dabei ist zu beachten, dass dieser Wert keine Angabe in Sekunden ist, sondern noch mit der Angabe von Allgemein/Aktualisierungsintervall multipliziert wird.
- Der Bereich Grids dient dazu die Grids (Tabellen) im imonc an die eigenen Bedürfnisse anzupassen. Einerseits kann für jedes Grid angegeben werden, welche Spalten angezeigt werden sollen, andererseits gibt es die Möglichkeit für die Grids im Bereich Anrufe, Verbindungen und Faxe anzugeben, von wann ab die Infos angezeigt werden sollen.

### 7.2.5. Seite Anrufe

Die Seite Calls wird nur angezeigt, wenn die Konfigurationsvariable TELMOND\_LOG auf 'yes' eingestellt ist, denn sonst wird kein Anruf-Log geführt. Auf dieser Seite werden alle abgespeicherten Telefonanrufe angezeigt, die eingegangen sind, während der Router eingeschaltet war. Dabei kann umgeschaltet werden zwischen der Ansicht der lokal gespeicherten Anrufe oder nur der auf dem Router gespeicherten Anrufe. Wird bei der Anzeige der auf dem Router gespeicherten Anrufe der Zurücksetzen-Button gedrückt, wird das Logfile auf dem Router gelöscht.

In der Anruf-Übersicht kann mit der rechten Maustaste auf der Rufnummer oder der eigenen MSN diese ins Telefonbuch übernommen werden, um der Rufnummer bzw. MSN dort einen Namen zuzuweisen, der dann stattdessen angezeigt wird.

### 7.2.6. Seite Verbindungen

Neu ist ab der Version 1.4 die Anzeige der vom Router aufgebauten Verbindungen zum Internet. Diese befindet sich auf der Seite Connections. Somit hat man einen guten Überblick, wie sich der Router bei der automatischen Einwahl ins Internet verhält. Damit diese Seite angezeigt werden kann, muss in der Datei config/base.txt die Variable IMOND\_LOG auf 'YES' gesetzt werden.

Genauso wie bei der Anruf-Übersicht kann auch hier zwischen den lokal gespeicherten und auf dem Router gespeicherten Verbindungen umgeschaltet werden. In der Ansicht der auf dem

Router gespeicherten Verbindungen bewirkt ein Drücken des Zurücksetzen-Buttons, dass das Logfile auf dem Router gelöscht wird.

Angezeigt werden pro Verbindung

- Provider
- Startdatum und -zeit
- Enddatum und -zeit
- Onlinezeit
- Abrechnungszeit
- entstandene Kosten
- empfangene Zeichen
- gesendete Zeichen

### 7.2.7. Seite Fax

Damit die Seite Faxe angezeigt wird, muss auf dem Router entweder das `OPT_MGETTY` von Michael Heimbach oder `OPT_MGETTY` von Felix Eckhofer installiert werden. Diese gibt es auf der fli4l-Homepage unter OPT-Pakete. Auf dieser Seite werden dann alle eingegangenen Faxe aufgelistet. Das Kontextmenü der Übersicht bietet mehrere Möglichkeiten, diese stehen allerdings nur im Admin-Modus zur Verfügung:

- Es kann ein Fax angezeigt werden. Dazu muss unter Admin/Remoteupdate der Pfad für das fli4l-Verzeichnis korrekt gesetzt werden, da die Faxe auf dem Router in gepackter Form vorliegen und somit gzip aus dem fli4l-Paket benötigt wird. Alternativ kann gzip.exe und win32gnu.dll auch ins imonc-Verzeichnis kopiert werden. Kann gzip.exe nicht an einer der beiden Stellen gefunden werden, wird stattdessen der Webserver des Routers probiert zu öffnen (direkt mit dem Aufruf des richtigen CGIs).
- Ein einzelnes Fax kann gelöscht werden. Dabei wird das Fax sowohl lokal als auch auf dem Router gelöscht (sowohl die eigentliche Faxdatei, als auch der Eintrag in den Logdateien).
- Sämtliche auf dem Router befindlichen Faxe löschen. Damit werden die Faxe und die Logdatei auf dem Router gelöscht. Die Faxe werden nicht aus der lokalen Logdatei gelöscht.

Genauso wie bei der Anruf-Übersicht kann auch hier zwischen den lokal gespeicherten und auf dem Router gespeicherten Faxen umgeschaltet werden.

### 7.2.8. Seite E-Mail

Diese Seite wird nur angezeigt, wenn im Config-Dialog mindestens ein aktiviertes POP3-E-Mail-Konto eingerichtet worden ist.

Die Seite E-Mail dürfte sich eigentlich selber erklären. Hiermit wird der mittlerweile eingebaute E-Mail-Checker beobachtet. Ist die Option "Check even if the router is offline" nicht

aktiviert, überprüft der E-Mail-Checker alle E-Mail-Konten nach E-Mails, sobald der Router online ist und anschließend im eingestellten Intervall. Ist die genannte Option aktiviert, überprüft der E-Mail-Checker im eingestellten Intervall. Ist der Router gerade online, wird die bestehende Verbindung benutzt. Ist er nicht online, wird eine Verbindung selbständig mit dem ausgewählten Circuit hergestellt, die, sobald alle E-Mail-Konten abgearbeitet sind, wieder getrennt wird. Damit man diese Option nutzen kann, muss Dialmode auf "auto" stehen.

Sind E-Mails auf dem POP3-Server vorhanden, wird entweder automatisch der eingestellte E-Mail-Client gestartet oder ein neues Symbol im Tray neben der Uhr angezeigt, welches als Hint die Anzahl der E-Mails auf jedem Server liefert. Ein Doppelclick startet dann den eingestellten E-Mail-Client. Ist ein Fehler bei einem der E-Mail-Konten aufgetreten, erscheint einerseits ein Hinweis in der E-Mail-History, andererseits wird das E-Mail-TrayIcon angezeigt, welches dadurch gekennzeichnet ist, dass die obere rechte Ecke rot gefärbt ist.

In der E-Mail-Übersicht kann man mit dem Kontextmenü Mails direkt auf dem Server löschen, ohne sie vorher komplett downloaden zu müssen. Dies geschieht, indem mit der rechten Maustaste das Kontextmenü angezeigt wird. Dabei sollte eine Zelle der entsprechenden Zeile markiert sein, wo die zu löschende E-Mail eingetragen ist. Im Kontextmenü wählt man den einzige Punkt Delete MailMessage aus.

### 7.2.9. Admin

Dieser Abschnitt steht nur zur Verfügung, wenn sich imonc im Admin-Modus befindet.

Der erste Punkt liefert eine Übersicht über die verwendeten Circuits – sprich Internetprovider – die der Router automatisch per LCR auswählt. Ein Doppelclick auf einen Provider in der Providerübersicht zeigt an, für welche Zeiträume der Circuit in config/base.txt definiert worden ist.

Der zweite Punkt dort ist die Möglichkeit ein Fernupdate auf dem Router einzuspielen. Dabei kann ausgewählt werden, welche fünf Programmpakete (Kernel, Rootfilesystem, Opt-Datei, rc.cfg und syslinux.cfg) auf den Router kopiert werden sollen. Damit man das Update einspielen kann, muss man zuerst mal das fli4l-Verzeichnis angeben, damit imonc weiss, woher es die nötigen Dateien nehmen soll. Ausserdem muss angegeben werden, in welchem Unterverzeichnis die Konfigurationsdateien liegen (standardmäßig config), um die Opt-Datei, rc.cfg und syslinux.cfg jeweils neu zu erzeugen. Es ist ratsam, einen Reboot nach dem Einspielen des Updates durchführen, damit die Änderungen auch direkt wirksam werden. Wird während des Updates nach einem Passwort nachgefragt, ist das Passwort gemeint, welches in config/base.txt unter PASSWORD eingetragen ist.

Um die Beschränkung des Port-Forwarding zu umgehen, dass ein Port nur an genau einen Client-Rechner gebunden ist, besteht jetzt die Möglichkeit, die Konfiguration auf dem Router zu editieren. Damit die Änderungen aktiv werden, muss die Verbindung neu hergestellt werden. Da die Datei nur in der Ramdisk ersetzt wird, bleiben die Änderungen nur bis zum nächsten Neustart des Routers erhalten. Um die Änderungen dauerhaft zu speichern, muss ein neues Opt-File auf dem Router installiert werden mit einer geeignet angepassten base.txt aus dem Config-Verzeichnis.

Der vierte Punkt auf der Admin-Seite – Dateien – dient dazu, Konfigurations- und Logdateien des Routers einfach per Maus-Click anzuzeigen. Die Auswahlliste wird über den Punkt Config/Admin und dort "files on router to view" konfiguriert. Anschliessend kann einfach über die ComboBox auf dieser Seite ausgewählt werden, welche Datei angezeigt werden soll.

Der fünfte Punkt ist die Seite DynEisfairLog, sie erscheint nur wenn im Config-Dialog unter



Admin die Zugangsdaten des DynEisfair-Accounts eingetragen worden sind. Ist dies geschehen, wird auf dieser Seite Log des Dienstes angezeigt.

Als letzten Punkt gibt es noch die Seite Hosts. Hier werden alle in der Datei `/etc/hosts` eingetragenen Rechner angezeigt. Weiterhin wird probiert jeden dieser dort eingetragenen Rechner anzupingen und das Ergebnis davon wird ebenfalls angezeigt. Somit kann man schnell rausbekommen, welche dieser Rechner eingeschaltet sind.

### 7.2.10. Seiten Fehler, Syslog und Firewall

Die Seiten Fehler, Syslog und Firewall werden nur angezeigt, wenn in den entsprechenden Logs Einträge vorhanden sind. Die Einträge der Seiten Syslog und Firewall werden nur angezeigt, wenn man im Admin-Modus ist.

Auf der Seite Fehler werden sämtliche imonc/imond-spezifischen Fehler festgehalten. Wenn Probleme bestehen, kann unter Umständen ein Blick auf diese Seite die Ursache der Probleme anzeigen.

Auf der Seite Syslog werden die ankommende Syslog-Meldungen angezeigt, bis auf die Meldungen der Firewall. Diese werden auf der eigenen Seite Firewall dargestellt. Damit dies funktioniert, muss die Variable `OPT_SYSLOGD` in der Konfigurationsdatei `config/base.txt` auf 'yes' gesetzt werden. Ausserdem muss die Variable `SYSLOGD_DEST` auf die IP des Clients gesetzt werden (genau: `SYSLOGD_DEST='@100.100.100.100` – wobei die IP natürlich an die IP des Clients angepasst werden muss). Angezeigt wird neben der eigentlichen Syslog-Meldung auch Datum, Uhrzeit, IP des Senders und die Prioritätsstufe.

Damit die Firewall-Meldungen bei den ganzen Syslog-Meldungen nicht untergehen, werden diese auf der separaten Seite Firewall angezeigt. Damit die Firewall-Meldungen angezeigt werden können, muss zusätzlich in der Datei `config/base.txt` die Konfigurationsvariable `OPT_KLOGD` auf 'yes' gesetzt werden.

### 7.2.11. Seite News

Auf dieser Seite werden, vorausgesetzt die Option ist im Config-Bereich des Imonc aktiviert, die News, welche auf der fli4l-Homepage angezeigt werden, auch direkt im Imonc angezeigt werden. Dazu wird mittels des http-Protokolls die URL `http://www.fli4l.de/german/news.xml` abgerufen. Neben den News werden mittlerweile auch die fünf aktuellsten Opt-Pakete angezeigt. Dazu wird die URL `http://www.fli4l.de/german/imonc_opt_show.php` abgefragt. Außerdem wird in der Statusleiste vom Imonc die Überschriften der News alternierend angezeigt.

## 7.3. Unix/Linux-Client imonc

Für Linux gibt es mittlerweile 2 Versionen: eine textbasierte (imonc) und eine mit graphischer Oberfläche (ximonc). Den Source zu ximonc findet man im Verzeichnis `src`. Die Dokumentation für ximonc wird erst in der 1.5-Final-Version zur Verfügung stehen. Ein erfahrener Linux-User sollte aber mit den Sources keine Probleme haben.

Beschränken wir uns daher hier zunächst auf die textbasierte Version von imonc: Dieses ist ein curses-basiertes Programm, hat also keine graphische Oberfläche. Der Source liegt im Verzeichnis `unix`.

Installation:

## 7. Client-/Server-Schnittstelle imon

```
cd unix
make install
```

imonc wird dabei in /usr/local/bin installiert.  
Aufruf:

```
imonc hostname
```

Dabei ist als hostname der Name oder die IP-Adresse des fli4l-Routers anzugeben, also z.B.

```
imonc fli4l
```

imonc zeigt folgende Informationen:

- Datum/Uhrzeit des fli4l-Routers
- Momentan eingestellte Route
- Default-Route-Circuits
- ISDN-Kanäle

**Status** : Calling/Online/Offline

**Name** : Telefonnummer des Gegners oder Circuit-Name

**Time** : Online-Zeit

**Charge-Time** : Online-Zeit unter Berücksichtigung des Zeittaktes

**Charge** : Berechnete Kosten

Mögliche Kommandos sind:

Nr	Befehl	Bedeutung
0	quit	Programm beenden
1	enable	Aktivieren
2	disable	Deaktivieren
3	dial	Wählen
4	hangup	Einhängen
5	reboot	Neu booten
6	timetable	Zeittabelle ausgeben
7	dflt route	Neuen Default-Route-Circuit bestimmen
8	add channel	2. Kanal hinzuschalten
9	rem channel	2. Kanal deaktivieren

Zu den Kommandos im Einzelnen:

**0 – quit** Die Verbindung zum imond-Server wird abgebaut und das Programm beendet.

**1 – enable** Alle Circuits werden auf dialmode “auto” gestellt. Das ist auch der Default-Zustand von fli4l nach dem Booten. Das heisst, dass fli4l bei einem Verbindungsaufbauwunsch eines Rechners im Netz automatisch rauswählt.

**2 – disable** Alle Circuits werden auf dialmode “off” gestellt. Damit ist fli4l so gut wie tot, bis er mit dem Enable-Kommando wieder geweckt wird.

- 3 – dial** Manuelle Wahl auf dem Default-Route-Circuit. Ist eher für Testzwecke gedacht, da fli4l normalerweise automatisch wählt.
- 4 – hangup** Manuelles Einhängen: damit kann man dem automatischen Einhängen von fli4l zuvorkommen.
- 5 – reboot** fli4l wird neu gebootet. Ziemlich überflüssiges Kommando ...
- 6 – timetable** Es wird die Zeittabelle für die Default-Route-Circuits ausgegeben. Beispiel: s.o.
- 7 – default route circuit** Manuelles Wechseln des Default-Route-Circuits. Kann z.B. dann sinnvoll sein, wenn man das automatische LC-Routing von fli4l für eine Weile ausser Kraft setzen will, da einige Provider einen Zugriff auf das eigene Postfach nur über den eigenen Internet-Zugang erlauben.
- 8 – add channel** Hier kann der 2. ISDN-Kanal manuell hinzugeschaltet werden. Voraussetzung: `ISDN_CIRC_x_BUNDLING` ist 'yes'.
- 9 – remove channel** Abschalten des 2. ISDN-Kanals. Siehe auch "add channel".

Sonst gelten bei diesen Kommandos dieselben Bemerkungen wie für den Windows-imond-Client `imonc.exe`.

Noch zu bemerken ist: Ab fli4l-1.4 ist es nun auch möglich, auf dem fli4l-Router selbst einen "minimalisierten" imon-Client zu installieren, nämlich durch Setzen von `OPT_IMONC='yes'` im Paket `TOOLS`.

Damit kann man nun auch an der fli4l-Konsole bestimmte Einstellungen, z.B. Routing etc. mit `imonc` vornehmen. Achtung: Dieser Mini-`imonc` funktioniert nur auf dem fli4l-Router selbst! Auf einem Linux-/Unix- Client ist immer der "große Bruder" `unix/imonc` zu verwenden.

## 8. Entwickler-Dokumentation

Dieses Kapitel führt in die Aspekte von fli4l ein, die hauptsächlich für jene interessant sind, die mit dem Gedanken spielen, fli4l durch die Entwicklung eigener Pakete und OPTs zu erweitern. Es wird erläutert, wie fli4l „unter der Haube“ arbeitet und wie man in gewisse Prozesse eingreifen kann, um die Funktionalität von fli4l zu verändern oder zu verbessern.

### 8.1. Allgemeine Regeln

Damit ein neues Paket in die OPT-Datenbank auf der fli4l-Homepage aufgenommen wird, müssen einige Regeln beachtet werden. Pakete, die sich nicht an diese Regeln halten, können ohne Vorwarnung aus der Datenbank entfernt werden.

1. *Keine* Kopieraktionen von Seiten des Benutzers! fli4l bietet ein ausgefeiltes System, um die Daten der fli4l-Pakete in die Installationsarchive einzupacken. Alle Dateien, die auf den Router sollen, liegen im Verzeichnis `opt/`.
2. Pakete richtig packen und komprimieren: Die Pakete müssen so aufgebaut sein, dass sie sich mühelos ins fli4l-Verzeichnis entpacken lassen.
3. Die Pakete sollen sich *vollständig* über die Konfigurationsdatei konfigurieren lassen. Ein weiteres Bearbeiten der Konfigurationsdateien darf nicht vom Benutzer verlangt werden. Schwierige Entscheidungen dem Benutzer abnehmen oder in einen erweiterten Bereich verlagern (ans Ende der Konfigurationsdatei mit einem dicken Hinweis, etwa: ONLY MODIFY IF YOU KNOW WHAT YOU DO).
4. Noch ein Hinweis zur Konfigurationsdatei: Anhand des Namens einer Variablen muss sich eindeutig erkennen lassen, zu welchem OPT sie gehört. So gehören z. B. zum `OPT_HTTPD` die Variablen `OPT_HTTPD`, `HTTPD_USER_N`, usw.
5. Bitte, bitte, macht möglichst kleine Binaries (Programme)! Das passiert automatisch, wenn ihr das FBR aus dem *src*-Paket verwendet. Denkt auch daran, unnötige Features zu deaktivieren. Bei vorkompilierten Programmen hilft u. U. ein

```
strip -R .comment -R .note <Dateiname>
```

weiter. Nichts ist frustrierender als ein Download von 2 MiB, wenn man nachher feststellt, dass 500 kiB gereicht hätten...

**Wichtig:** *Bitte auf diese Art und Weise keine Kernel-Module behandeln! Sie werden hinterher nicht mehr funktionieren!*

6. Prüft euer Copyright! Wenn ihr Dateien als Vorlagen benutzt, achtet bitte darauf, das Copyright entsprechend zu ändern. Dies gilt besonders für die Config-, Check- und Opt-Textdateien. Ersetzt hier das Copyright durch euren eigenen Namen. Bei wortwörtlich kopierter Dokumentation muss natürlich das Copyright des Original-Autors erhalten bleiben!
7. Bitte als Archivtypen nur verbreitete, freie Formate benutzen. Dazu gehören:
  - ZIP (`.zip`)
  - GZIP (`.tgz` oder `.tar.gz`)

Andere Formate wie RAR, ACE, Blackhole, LHA etc. bitte nicht verwenden. Auch Windows-Installer-Dateien (`.msi`) oder selbstextrahierende Archive und Installer (`.exe`) sind nicht zu benutzen.

## 8.2. Übersetzen von Programmen

Die für das Übersetzen von Programmen zum Einsatz auf dem fli4l-Router erforderliche Umgebung wird im separat erhältlichen *src*-Paket angeboten. Dort wird auch dokumentiert, wie sich eigene Programme für den fli4l übersetzen lassen.

## 8.3. Modulkonzept

fli4l wird in Module (Pakete) aufgeteilt, u. a. in:

- *fli4l-4.0.0-trunk-rpi-r60784* ← Das Basis-Paket
- *dns\_dhcp*
- *dsl*
- *isdn*
- *sshd*
- und viele weitere...

Mit dem Basis-Paket ist fli4l ein reiner Ethernet-Router. Für ISDN und/oder DSL ist das Paket *isdn* und/oder *dsl* in dem fli4l-Verzeichnis auszupacken. Entsprechendes gilt für die anderen Pakete.

### 8.3.1. mkfli4l

Aus den Paketen werden in Abhängigkeit von der konkreten Konfiguration eine Konfigurationsdatei namens `rc.cfg` und zwei Archive namens `rootfs.img` und `opt.img` erstellt, die alle Konfigurationsinformationen und alle benötigten Dateien enthalten. Diese Dateien werden mit Hilfe von `mkfli4l` erzeugt, welches die einzelnen Pakete einliest und auf Fehler in der Konfiguration prüft.

`mkfli4l` akzeptiert die in Tabelle 8.1 angegebenen Parameter. Fehlen sie, werden die in Klammern angegebenen Werte angenommen. Eine vollständige Liste der Optionen (Tabelle 8.1) erhält man, wenn man

`mkfli41 -h`

aufruft.

Tabelle 8.1.: Parameter für `mkfli41`

Option	Bedeutung	
-c, --config	Setzen des Verzeichnisses, in dem <code>mkfli41</code> die config-Dateien der Pakete sucht (Standard: <code>config</code> )	
-x, --check	Setzen des Verzeichnisses, in dem <code>mkfli41</code> die zum Prüfen der Pakete benötigten Dateien sucht ( <code>&lt;package&gt;.txt</code> , <code>&lt;package&gt;.exp</code> und <code>&lt;package&gt;.ext</code> ; Standard: <code>check</code> )	
-l, --log	Setzen der Logdatei; <code>mkfli41</code> protokolliert Fehlermeldungen und Warnungen in dieser Datei (Standard: <code>img/mkfli41.log</code> )	
-p, --package	Angabe der Pakete, die geprüft werden sollen. Diese Option kann mehrmals angegeben werden, wenn man mehrere Pakete im Zusammenhang prüfen will. Bei Verwendung von <code>-p</code> wird allerdings grundsätzlich zuerst die Datei <code>&lt;check_dir&gt;/base.exp</code> eingelesen, um die allgemeinen regulären Ausdrücke, die vom Basis-Paket bereitgestellt werden, zur Verfügung zu stellen. Diese Datei muss also existieren.	
-i, --info	Gibt Auskunft über den Verlauf der Prüfung (welche Dateien werden gelesen, welche Prüfungen werden durchgeführt, welche besonderen Dinge traten während des Prüfprozesses auf)	
-v, --verbose	Ausführlichere Variante von <code>-i</code>	
-h, --help	Zeigt die Hilfe an	
-d, --debug	Erleichtert die Fehlersuche im Prüfprozess. Dies ist als Hilfe für Paketentwickler gedacht, die etwas genauer wissen möchten, wie die Prüfung des Paketes abläuft.	
	Debugoption	Bedeutung
	check	show check process
	zip-list	show generation of zip list
	zip-list-skipped	show skipped files
	zip-list-regexp	show regular expressions for ziplist
	opt-files	check all files in <code>opt/&lt;package&gt;.txt</code>
	ext-trace	show trace of extended checks

### 8.3.2. Aufbau

Ein Paket kann mehrere OPTs enthalten, wenn es aber nur eins enthält, ist es allerdings zweckmäßig, das Paket genauso wie das OPT zu nennen. Im Folgenden ist `<PAKET>` durch den jeweiligen Paket-Namen zu ersetzen. Ein Paket besteht aus folgenden Teilen:

- Verwaltungsdateien
- Dokumentation
- Entwickler-Dokumentation

- Client-Programme
- Quellcode
- Weitere Dateien

Die einzelnen Teile sind im Folgenden näher beschrieben.

### 8.3.3. Die Konfiguration der Pakete

In der Datei `config/<PAKET>.txt` werden vom Benutzer Änderungen an der Konfiguration des Pakets vorgenommen. Alle Variablen eines OPTs sollten einheitlich mit dem Namen des OPTs beginnen, also zum Beispiel:

```
#-----
# Optional package: TELNETD
#-----
OPT_TELNETD='no'      # install telnetd: yes or no
TELNETD_PORT='23'     # telnet port
```

Ein OPT sollte in der Konfigurationsdatei durch einen Header (siehe oben) entsprechend abgegrenzt werden. Dies erhöht die Übersichtlichkeit, zumal ein Paket ja auch mehrere OPTs enthalten kann. Die dem OPT zugehörigen Variablen sollten — ebenfalls im Interesse der Übersichtlichkeit — nicht weiter eingerückt werden. Kommentare und Leerzeilen sind erlaubt, wobei Kommentare einheitlich in Spalte 33 beginnen sollen. Ist eine Variable inklusive ihrer Belegung länger als 32 Zeichen, ist der Kommentar eine Zeile versetzt ab Spalte 33 einzufügen. Längere Kommentare werden jeweils ab Spalte 33 beginnend auf mehrere Zeilen aufgeteilt. Diese Maßnahmen sollen die Lesbarkeit der Konfigurationsdatei erhöhen.

Alle Werte hinter dem Gleichheitszeichen müssen in Hochkommata<sup>1</sup> eingefasst werden, da es sonst beim Booten zu Problemen kommen kann.

Variablen, die aktiv sind (s. u.), werden in die `rc.cfg` übernommen, alles andere wird ignoriert. Einzige Ausnahme sind Variablen mit dem Namen `<PAKET>_DO_DEBUG`. Diese dienen zur Fehlersuche in Paketen und werden pauschal übernommen.

### 8.3.4. Die Liste der zu kopierenden Dateien

Die Datei `opt/<PAKET>.txt` enthält Anweisungen, die beschreiben

- welche Dateien zu welchem OPT gehören,
- wann sie in das zu generierende `opt-` bzw. `rootfs-`Archiv übernommen werden sollen,
- welche UID<sup>2</sup>, GID<sup>3</sup> und Rechte<sup>4</sup> jede Datei bekommen soll,

<sup>1</sup>Es können sowohl einfache Hochkommata als auch doppelte Hochkommata verwendet werden. Man kann also `F00='bar'` oder auch `F00="bar"` schreiben. Die Verwendung von doppelten Hochkommata sollte allerdings die Ausnahme sein und man sollte sich vorher unbedingt darüber informieren, wie eine Unix-Shell mit einfachen und doppelten Hochkommata umgeht.

<sup>2</sup>User ID: Eigentümer der Datei

<sup>3</sup>Group ID: Gruppe der Datei

<sup>4</sup>Darf die Datei gelesen, beschrieben oder ausgeführt werden?

- welche Konvertierungen vor Aufnahme ins Archiv erfolgen sollen.

`mkfli4l` generiert darauf basierend die erforderlichen Archive.

Leere Zeilen und Zeilen, die mit `#` anfangen, werden ignoriert. In einer der ersten Zeilen sollte die Version des Paket-Dateiformats wie folgt stehen:

```
<erste Spalte>      <zweite Spalte> <dritte Spalte>
opt_format_version  1                -
```

Die restlichen Zeilen haben folgende Syntax:

```
<erste Spalte> <zweite Spalte> <dritte Spalte> <folgende spalten>
Variable       Wert           Datei          Optionen
```

1. In der ersten Spalte steht der Name einer Variable, von deren Wert das Übernehmen der in der dritten Spalte stehenden Datei abhängt. Der Name einer Variable kann beliebig oft in der ersten Spalte auftauchen, falls mehrere Dateien von ihr abhängen. Jede Variable, die in der Datei `opt/<PAKET>.txt` auftaucht, wird von `mkfli4l` markiert.

Falls mehrere Variablen auf denselben Wert geprüft werden sollen, kann auch eine Liste von Variablen (durch Kommata getrennt) verwendet werden. In diesem Falle reicht es aus, wenn mindestens *eine* Variable den in der zweiten Spalte geforderten Wert enthält. Wichtig ist dabei, dass zwischen den einzelnen Variablen *keine* Leerzeichen stehen!

Bei OPT-Variablen (also Variablen, die mit `OPT_` beginnen und typischerweise den Typ `YESNO` haben) kann das Präfix „`OPT_`“ weggelassen werden. Des Weiteren ist es unwichtig, ob Variablen in Groß- oder in Kleinbuchstaben (oder beliebig gemischt) notiert werden.

2. In der zweiten Spalte steht ein Wert. Stimmt die in der ersten Spalte stehende Variable mit diesem Wert überein und ist die Variable aktiv (s. u.), wird die Datei in der dritten Spalte übernommen. Steht eine %-Variable in der ersten Spalte, wird über alle Indizes iteriert und geprüft, ob irgendein Element des Arrays mit dem Wert übereinstimmt. Ist das der Fall, wird kopiert. Zusätzlich wird vermerkt, dass aufgrund des aktuellen Wertes der Variable eine Datei kopiert wurde.

Es ist möglich, vor den Wert ein „!“ zu schreiben. In diesem Falle wird die Prüfung negiert, d. h. die Datei wird genau dann kopiert, wenn die Variable diesen Wert *nicht* enthält.

3. In der dritten Spalte steht der Name einer Datei. Die Pfadangabe erfolgt relativ zum `opt`-Verzeichnis. Die Datei muss existieren und lesbar sein, sonst gibt es beim Generieren der Archive einen Fehler und die Generierung wird abgebrochen.

Beginnt der Dateiname mit `rootfs:`, wird die Datei in die Liste der ins `rootfs`-Archiv aufzunehmenden Dateien übernommen. Der Präfix wird vorher entfernt. Taucht dieselbe Datei sowohl mit als auch ohne `rootfs:`-Präfix auf, wird sie nur ins `rootfs`-Archiv übernommen.

Liegt die Datei unterhalb des verwendeten Konfigurationsverzeichnisses, wird sie in die Liste der aus dem Konfigurationsverzeichnis zu übernehmenden Dateien aufgenommen, andernfalls wird die unter `opt/` liegende Datei genommen.



Ist die zu kopierende Datei ein Kernel-Modul, kann man die konkrete Kernel-Version durch `${KERNEL_VERSION}` ersetzen. `mkfli41` nimmt dann die Version aus der Konfiguration und setzt sie hier ein. Dadurch kann man einem Paket Module für verschiedene Kern-Versionen mitgeben und es wird immer die für den Kern richtige Version mit auf den Router kopiert. Für Kernel-Module kann der Pfad auch vollkommen entfallen. `mkfli41` findet das Modul anhand der Dateien `modules.dep` und `modules.alias`, siehe Abschnitt „Automatische Auflösung von Abhängigkeiten für Kernel-Module“ (Seite 348).

4. In den anderen Spalten können die in Tabelle 8.2 aufgeführten Optionen für den Eigentümer, die Gruppe, die Rechte der Dateien und Konvertierungen stehen.

Einige Beispiele:

- kopiere Datei, wenn `OPT_TELNETD='yes'`, setze UID/GID auf root und die Rechte auf 755 (`rw-r-xr-x`):

```
telnetd      yes      usr/sbin/in.telnetd mode=755
```

- kopiere Datei (`OPT_BASE='yes'` gilt implizit immer); setze UID/GID auf root, die Rechte auf 555 (`r-xr-xr-x`) und konvertiere die Datei ins Unix-Format bei gleichzeitigem Entfernen aller überflüssigen Zeichen:

```
base        yes      etc/rc0.d/rc500.killall mode=555 flags=sh
```

- kopiere Kernel-Modul, wenn `PCMCIA_PCIC='i82365'`; setze UID/GID auf root und die Rechte auf 644 (`rw-r--r--`):

```
pcmcia_pcic i82365 lib/modules/${KERNEL_VERSION}/pcmcia/i82365.ko
```

- kopiere Kernel-Modul, wenn `PCMCIA_PCIC='i82365'`; setze UID/GID auf root und die Rechte auf 644 (`rw-r--r--`) (alternative Form):

```
pcmcia_pcic i82365 i82365.ko
```

- kopiere Kernel-Modul, wenn mindestens einer der Einträge in `NET_DRV_%` den Wert 3c503 besitzt; setze UID/GID auf root und die Rechte auf 644 (`rw-r--r--`):

```
net_drv_%    3c503    3c503.ko
```

- kopiere Datei, wenn die Variable `POWERMANAGEMENT` *nicht* den Wert „none“ enthält:

```
powermanagement !none etc/rc.d/rc100.pm mode=555 flags=sh
```

- kopiere Datei, wenn irgendeine der OPT-Variablen `OPT_MYOPTA` oder `OPT_MYOPTB` den Wert „yes“ enthält:

```
myopta,myoptb yes  usr/local/bin/myopt-common.sh mode=555 flags=sh
```

Tabelle 8.2.: Optionen für Dateien

Option	Bedeutung	Standardwert
type=	<p>Der Typ des Eintrags:</p> <p><i>local</i>     Dateisystem-Objekt  <i>file</i>       Datei  <i>dir</i>        Verzeichnis  <i>node</i>       Gerät  <i>symlink</i>   (symbolische) Verknüpfung</p> <p>Wenn vorhanden, muss diese Option an erster Stelle stehen. Der Typ „local“ steht hierbei für den Typ eines im Dateisystem existierenden Objekts und entspricht somit „file“, „dir“, „node“ oder „symlink“ (je nachdem). Die anderen Typen mit Ausnahme von „file“ können Einträge im Archiv erzeugen, die nicht im lokalen Dateisystem vorliegen müssen. Das wird z. B. benutzt, um Gerätedateien im <b>rootfs</b>-Archiv anzulegen.</p>	local
uid=	Der Eigentümer der Datei, entweder numerisch oder als Name aus passwd	root
gid=	Die Gruppe der Datei, entweder numerisch oder als Name aus group	root
mode=	Die Zugriffsrechte	<p>Dateien und Geräte:  <b>rw-r--r--</b> (644)  Verzeichnisse:  <b>rwxr-xr-x</b> (755)  Verknüpfungen:  <b>rwxrwxrwx</b> (777)</p>
flags= (type=file)	<p>Konvertierungen vor der Aufnahme ins Archiv:</p> <p><i>utxt</i>    Konvertierung ins Unix-Format  <i>dtxt</i>    Konvertierung ins DOS-Format  <i>sh</i>      Shell-Skript: Konvertierung ins Unix-Format, Entfernen überflüssiger Zeichen  <i>luac</i>    Lua-Skript: Übersetzung in Bytecode der Lua-VM</p>	
name=	Alternativer Name, unter dem der Eintrag ins Archiv aufgenommen wird	
devtype= (type=node)	Beschreibt den Typ des Geräts („c“ für zeichenorientierte und „b“ für blockorientierte Geräte). Muss an zweiter Stelle stehen.	
major= (type=node)	Beschreibt die so genannte „Major“-Nummer der Gerätedatei. Muss an dritter Stelle stehen.	
minor= (type=node)	Beschreibt die so genannte „Minor“-Nummer der Gerätedatei. Muss an vierter Stelle stehen.	
linktarget= (type=symlink)	Beschreibt das Ziel der symbolischen Verknüpfung. Muss an zweiter Stelle stehen.	

Dieses Beispiel ist letztlich nur eine Kurzschreibweise für:

```
myopta yes usr/local/bin/myopt-common.sh mode=555 flags=sh
myoptb yes usr/local/bin/myopt-common.sh mode=555 flags=sh
```

Und letzteres ist eine Kurzschreibweise für:

```
opt_myopta yes usr/local/bin/myopt-common.sh mode=555 flags=sh
opt_myoptb yes usr/local/bin/myopt-common.sh mode=555 flags=sh
```

- kopiere Datei `opt/usr/bin/beep.sh` ins `rootfs`-Archiv, aber benenne sie vorher in `bin/beep` um:

```
base yes rootfs:usr/bin/beep.sh mode=555 flags=sh name=bin/beep
```

Wenn im Paket eine Variable referenziert wird, die nicht vom Paket selbst definiert wird, kann es passieren, dass das entsprechende Paket nicht installiert ist. Das führt für gewöhnlich zu einer Fehlermeldung in `mkfli41`, da `mkfli41` erwartet, dass alle von `opt/<PAKET>.txt` referenzierten Variablen definiert sind.

Um diese Situation korrekt handhaben zu können, wurde die „weak“-Deklaration eingeführt. Sie hat das folgende Format:

```
weak      <Variable>      -
```

Dadurch wird die Variable definiert und ihr Wert intern auf „undefiniert“ gesetzt, wenn sie nicht bereits definiert worden ist. Dabei ist jedoch zu beachten, dass hier das „`OPT_`“-Präfix *nicht* weggelassen werden darf (falls es existiert), weil sonst eine Variable *ohne* dieses Präfix definiert wird.

Ein Beispiel aus der `opt/rrdtool.txt`:

```
weak opt_openvpn -
[...]
openvpn    yes    usr/lib/collectd/openvpn.so
```

Ohne die `weak`-Definition würde `mkfli41` bei der Nutzung des Pakets „`rrdtool`“ eine Fehlermeldung anzeigen, wenn das „`openvpn`“-Paket nicht ebenfalls vorliegt. Mit Hilfe der `weak`-Definition kommt auch in dem Fall, dass das „`openvpn`“-Paket nicht vorliegt, keine Fehlermeldung.

## Konfigurations-spezifische Dateien

In manchen Situationen möchte man originale Dateien im `opt`- oder `rootfs`-Archiv durch Konfigurations-spezifische Dateien wie z.B. Host-Keys, eigene Firewall-Skripte, ... ersetzen. `mkfli41` unterstützt dieses Szenario, indem es prüft, ob eine zu kopierende Datei im Konfigurationsverzeichnis zu finden ist, und übernimmt in diesem Falle diese Datei in die Liste der ins Archiv aufzunehmenden Dateien.

Eine weitere Möglichkeit, Konfigurations-spezifische Dateien ins Archiv aufzunehmen, wird im Abschnitt [„Erweiterte Prüfungen der Konfiguration“](#) (Seite 366) beschrieben.

### Automatische Auflösung von Abhängigkeiten für Kernel-Module

Kernel-Module bauen unter Umständen auf anderen Kernel-Modulen auf. Diese müssen vor ihnen geladen werden und daher gleichfalls in das Archiv aufgenommen werden. `mkfli4l` bestimmt diese Abhängigkeiten anhand von `modules.dep` und `modules.alias`, zweier beim Kernel-Bauen generierter Dateien, und nimmt automatisch alle benötigten Module in die Archive auf. So führt z. B. folgender Eintrag

```
net_drv_%    ne2k-pci    ne2k-pci.ko
```

dazu, dass auch `8390.ko` ins Archiv aufgenommen wird, da `ne2k-pci.ko` davon abhängt.

Die notwendigen Einträge in `modules.dep` und `modules.alias` werden in das `rootfs`-Archiv mit aufgenommen und können von `modprobe` zum Laden der Treiber genutzt werden.

#### 8.3.5. Die Prüfung der Konfiguration-Variablen

Mit Hilfe der Datei `check/<PAKET>.txt` können die Inhalte der Variablen auf Gültigkeit überprüft werden. Diese Überprüfung war in früheren Versionen fest im Programm `mkfli4l` eingebaut, wurde aber im Zuge der Modularisierung von `fli4l` in die Check-Dateien ausgelagert. In dieser Datei ist für jede Variable aus den Konfigurationsdateien eine Zeile vorhanden. Diese Zeilen bestehen aus vier bis fünf Spalten, welche folgende Funktionen haben:

1. Variable: Diese Spalte gibt den Namen der zu überprüfenden Variable aus der Konfigurationsdatei an. Wenn es sich dabei um eine so genannte *Array-Variable* handelt, die mehrmals mit verschiedenen Indizes auftauchen kann, wird an Stelle der Nummer ein Prozentzeichen (%) in den Variablenname eingefügt. Dieses wird immer als „\_%\_“ in der Mitte eines Namens bzw. „\_%“ am Ende eines Namens verwendet. Der Name kann dabei mehrere Prozentzeichen enthalten, so dass man auch mehrdimensionale Arrays realisieren kann. Dann sollte zwischen den Prozentzeichen allerdings etwas stehen, muss aber nicht, was dann allerdings zu so seltsamen Namen wie „FOO\_%\_%“ führt.

Oftmals hat man das Problem, dass bestimmte Variablen Optionen beschreiben, die man nur in bestimmten Situationen benötigt. Deshalb können Variablen als optional markiert werden. Optionale Variablen werden mit einem vorangestellten „+“ gekennzeichnet. Sie können dann da sein, müssen aber nicht. Arrays können auch mit einem „++“ Präfix versehen werden. Steht ein „+“ davor, kann das Array da sein oder ganz fehlen. Steht „++“ davor, können zusätzlich auch noch einzelne Elemente des Arrays fehlen.

2. OPT\_VARIABLE: Diese Spalte teilt die Variable einem bestimmten OPT zu. Die Variable wird nur auf Gültigkeit überprüft, wenn die hier angegebene Variable auf „yes“ steht. Gibt es keine OPT-Variable, ist hier ein „-“ anzugeben. In diesem Fall muss die Variable in der Konfigurationsdatei definiert werden, es sei denn, es wird eine Standard-Belegung definiert (s. u.). Der Name der OPT-Variable kann beliebig sein, er sollte jedoch mit dem Präfix „OPT\_“ beginnen.

Falls eine Variable von keiner OPT-Variablen abhängt, gilt sie als *aktiv*. Falls sie von einer OPT-Variablen abhängig ist, ist sie genau dann aktiv, wenn

- ihre OPT-Variable aktiv ist und
- ihre OPT-Variable den Wert „yes“ enthält.

Andernfalls ist die Variable inaktiv.

**Hinweis:** Inaktive OPT-Variablen werden, wenn sie in der Konfiguration mit „yes“ belegt werden, auf den Wert „no“ zurückgesetzt; dies wird von `mkfli4l` auch mit einer entsprechenden Warnmeldung (bspw. „OPT\_Y='yes' ignored, because OPT\_X='no'“) kommentiert. Bei transitiven Abhängigkeitsketten (OPT\_Z hängt von OPT\_Y ab, das wiederum von OPT\_X abhängt) funktioniert dies aber nur dann zuverlässig, wenn die Namen aller OPT-Variablen mit „OPT\_“ beginnen.

3. **VARIABLE\_N:** Steht in der ersten Spalte eine Variable mit einem % im Namen, wird hier die Variable angegeben, die die Häufigkeit des Auftretens der Variable beschreibt (die so genannte *N-Variable*). Ist die Variable mehrdimensional, wird die Häufigkeit des letzten Index beschrieben. Hängt die Variable von einem OPT ab, muss die N-Variable vom selben OPT oder von keinem OPT abhängig sein. Ist die Variable von keinem OPT abhängig, darf auch die N-Variable von keinem OPT abhängig sein. Gibt es keine N-Variable, ist hier ein „-“ anzugeben.

Aus Kompatibilitätsgründen mit zukünftigen `fli4l`-Versionen *muss* die hier angegebene Variable identisch sein mit der Variable in `OPT_VARIABLE`, wobei das letzte „%“ durch ein „N“ ersetzt und alles dahinter entfernt wurde. Ein Array `HOST_%_IP4` bekommt also zwingend die N-Variable `HOST_N` zugewiesen und ein Array `PF_USR_CHAIN_%_RULE_%` also die N-Variable `PF_USR_CHAIN_%_RULE_N`, und diese N-Variable ist selbst wieder eine Array-Variable mit der zugehörigen N-Variable `PF_USR_CHAIN_N`. *Alle anderen Benennungen der N-Variable werden mit zukünftigen fli4l-Versionen inkompatibel sein!*

4. **VALUE:** Diese Spalte gibt an, welche Werte für diese Variable eingegeben werden können. Es sind dabei z. B. folgende Angaben möglich:

Name	Bedeutung
NONE	Es wird keine Überprüfung vorgenommen
YESNO	Die Variable muss „yes“ oder „no“ sein
NOTEMPTY	Die Variable darf nicht leer sein
NOBLANK	Die Variable darf kein Leerzeichen enthalten
NUMERIC	Die Variable muss numerisch sein
IPADDR	Die Variable muss eine IP-Adresse sein
DIALMODE	Die Variable muss „on“, „off“ oder „auto“ sein

Werden die Werte mit einem „WARN\_“-Präfix versehen, so führt ein illegaler Wert nicht zu einer Fehlermeldung und damit zu einem Abbruch von `mkfli4l`, sondern nur zur Ausgabe einer Warnung.

Die möglichen Prüfungen werden durch reguläre Ausdrücke in `check/base.exp` definiert. Diese Datei kann erweitert werden und enthält neuerdings z. B. zusätzlich folgende Prüfungen: `HEX`, `NUMHEX`, `IP_ROUTE`, `DISK` und `PARTITION`.

Die Anzahl der Ausdrücke kann jederzeit erweitert werden, hier ist Rückmeldung von den Paket-Entwicklern erforderlich.

Zusätzlich können reguläre Ausdrücke auch direkt in den Check-Dateien angegeben werden, wobei man auch Bezug auf existierende Ausdrücke nehmen kann. Statt `YESNO` könnte man z. B. auch

```
RE:yes|no
```

schreiben. Sinnvoll ist es dann, wenn ein Test nur ein einziges Mal ausgeführt wird und relativ einfach ist. Für genauere Informationen siehe nächstes Kapitel.

5. Standard-Belegung: In dieser Spalte kann optional ein Standard-Wert für die Variable stehen, falls die Variable nicht in der Konfiguration steht.

**Hinweis:** Dies funktioniert zur Zeit jedoch nicht für Array-Variablen. Auch darf die Variable nicht optional sein, es darf also kein „+“ vor dem Variablennamen stehen.

Beispiel:

```
OPT_TELNETD      -      -      YESNO      "no"
```

Fehlt OPT\_TELNETD nun in der Konfigurationsdatei, wird „no“ angenommen und dieser Wert auch in die `rc.cfg` geschrieben.

Die Sache mit dem Prozentzeichen lässt sich am Besten mit einem Beispiel erklären. Nehmen wir an, in der `check/base.txt` steht:

```
NET_DRV_N      -      -      NUMERIC
NET_DRV_%      -      NET_DRV_N      NONE
NET_DRV_%_OPTION  -      NET_DRV_N      NONE
```

Das heißt, dass je nach Wert von NET\_DRV\_N die Variablen NET\_DRV\_N, NET\_DRV\_1\_OPTION, NET\_DRV\_2\_OPTION, NET\_DRV\_3\_OPTION, usw. überprüft werden.

### 8.3.6. Eigene Definitionen zum Prüfen der Konfigurationsvariablen

#### Einführung regulärer Ausdrücke

In der Version 2.0 gab es nur die oben angeführten sieben Werte-Bereiche, auf die Variablen geprüft werden können: NONE, NOTEMPTY, NUMERIC, IPADDR, YESNO, NOBLANK, DIALMODE. Die Überprüfung war in `mkf1i41` fest eingebaut, nicht erweiterbar und beschränkte sich auf wesentliche „Datentypen“, die mit vertretbarem Aufwand geprüft werden können.

Mit der Version 2.1 wurde diese Prüfung neu implementiert. Ziel der neuen Implementierung ist eine flexiblere Prüfung der Variablen, die auch in der Lage ist, komplexere Ausdrücke zu prüfen. Deshalb werden reguläre Ausdrücke verwendet, die in einem oder mehreren separaten Dateien abgespeichert werden. Dadurch wird es zum einen möglich, Variablen zu prüfen, die im Augenblick noch nicht geprüft werden, und zum anderen können Entwickler optionaler Pakete eigene Ausdrücke definieren, um die Konfiguration ihrer Pakete prüfen zu lassen.

Eine Beschreibung regulärer Ausdrücke findet man via „man 7 regex“ oder z. B. hier: <http://unixhelp.ed.ac.uk/CGI/man-cgi?regex+7>.

#### Spezifikation regulärer Ausdrücke

Spezifizieren kann man die Ausdrücke auf zwei Wegen:

1. Paketspezifische exp-Datei `check/<PAKET>.exp`

Diese Datei liegt im `check`-Verzeichnis und trägt den gleichen Namen wie das dazugehörige Paket, also z. B. `check/base.exp`. Sie enthält Definitionen für Ausdrücke, die in der Datei `check/<PAKET>.txt` referenziert werden können. So enthält `check/base.exp` im

Augenblick Definitionen für die bekannten Prüfungen und `check/isdn.exp` eine Definition für die Variable `ISDN_CIRC_x_ROUTE` (das Fehlen dieser Überprüfung war der Auslöser dieser Änderungen).

Die Syntax lautet wie folgt, wobei man auch hier bei Bedarf doppelte Hochkommata verwenden kann:

```
<Name> = '<Regulärer Ausdruck>' : '<Fehlermeldung>'
```

oder am Beispiel aus `check/base.exp`:

```
NOTEMPTY = '.*[~ ]+.*'           : 'should not be empty'
YESNO     = 'yes|no'              : 'only yes or no are allowed'
NUMERIC   = '0|[1-9][0-9]*'       : 'should be numeric (decimal)'
OCTET     = '1?[0-9]?[0-9]|2[0-4][0-9]|25[0-5]'
           : 'should be a value between 0 and 255'
IPADDR    = '((RE:OCTET)\.){3}(RE:OCTET)' : 'invalid ipv4 address'
EIPADDR    = '()|(RE:IPADDR)'
           : 'should be empty or contain a valid ipv4 address'
NOBLANK   = '[^ ]+'              : 'should not contain spaces'
DIALMODE  = 'auto|manual|off'     : 'only auto, manual or off are allowed'
NETWORKS  = '(RE:NETWORK)([[:space:]]+(RE:NETWORK))*'
           : 'no valid network specification, should be one or more
             network address(es) followed by a netmask,
             for instance 192.168.6.0/24'
```

In den regulären Ausdrücken können auch Referenzen auf bereits existierende Definitionen enthalten sein. Diese werden dann einfach an der Stelle eingefügt. Dadurch ist es einfacher, reguläre Ausdrücke zu konstruieren. Eingefügt werden die Referenzen einfach durch `'(RE:Referenz)'`. (Siehe die Definition des Ausdrucks `NETWORKS` oben für ein entsprechendes Beispiel.)

Die Fehlermeldungen tendieren dazu, zu lang zu werden. Daher besteht die Möglichkeit, sie über mehrere Zeilen zu verteilen. Die folgenden Zeilen müssen dann immer mit einem Leerzeichen oder Tabulator beginnen. Beim Einlesen der `check/<PAKET>.exp`-Datei werden überflüssige Leerzeichen auf eins reduziert und Tabulatoren durch Leerzeichen ersetzt. Ein Eintrag in der `check/<PAKET>.exp` könnte dann so aussehen:

```
NUM_HEX      = '0x[[:xdigit:]]+'
              : 'should be a hexadecimal number
                (a number starting with "0x")'
```

## 2. Reguläre Ausdrücke direkt in der Check-Datei `check/<PAKET>.txt`

Manche Ausdrücke kommen nur einmal vor, dann lohnt es sich nicht, dafür einen regulären Ausdruck in einer `check/<PAKET>.exp`-Datei zu definieren. Dann kann man diesen Ausdruck einfach in die Check-Datei schreiben, z. B.:

# Variable	OPT_VARIABLE	VARIABLE_N	VALUE
MOUNT_BOOT	-	-	RE:ro rw no

MOUNT\_BOOT kann lediglich die Werte „ro“, „rw“ oder „no“ annehmen, alles andere wird abgelehnt.

Will man Bezug auf existierende reguläre Ausdrücke nehmen, fügt man einfach eine Referenz via „(RE:...“ ein. Beispiel:

# Variable	OPT_VARIABLE	VARIABLE_N	VALUE
LOGIP_LOGDIR	OPT_LOGIP	-	RE:(RE:ABS_PATH) auto

### Erweiterung existierender regulärer Ausdrücke

Fügt ein optionales Paket einen zusätzlichen Wert für eine Variable hinzu, die von einem regulären Ausdruck geprüft wird, muss der reguläre Ausdruck erweitert werden. Dies geschieht einfach durch Definition der neuen möglichen Werte durch einen regulären Ausdruck (wie oben beschrieben) und Ergänzung des bestehenden regulären Ausdrucks in einer eigenen `check/<PAKET>.exp`-Datei. Dass ein bestehender Ausdruck modifiziert werden soll, kennzeichnet ein führendes „+“. Der neue Ausdruck ergänzt den bestehenden Ausdruck, indem der neue Wert als Alternative an den bestehenden Wert angehängt wird. Verwendet ein anderer Ausdruck den ergänzten Ausdruck, gilt auch dort die Ergänzung. Die angegebene Fehlermeldung wird einfach an die vorhandene hinten angehängt.

Am Beispiel der Ethernet-Treiber könnte das wie folgt aussehen:

- Das Basis-Paket stellt eine Menge von Ethernet-Treibern bereit und prüft die Variable `NET_DRV_x` mit dem regulären Ausdruck `NET_DRV`, der wie folgt spezifiziert ist:

```
NET_DRV          = '3c503|3c505|3c507|...'
                  : 'invalid ethernet driver, please choose one'
                  ' of the drivers in config/base.txt'
```

- Das Paket „pcmcia“ stellt jetzt zusätzliche Gerätetreiber bereit, muss also `NET_DRV` ergänzen. Das sieht dann wie folgt aus:

```
PCMCIA_NET_DRV   = 'pcnet_cs|xirc2ps_cs|3c574_cs|...' : ''
+NET_DRV          = '(RE:PCMCIA_NET_DRV)' : ''
```

Nun kann man zusätzlich auch noch PCMCIA-Treiber auswählen.

### Regulären Ausdruck in Abhängigkeit von YESNO-Variablen erweitern

Wenn man `NET_DRV` wie oben um die PCMCIA-Treiber erweitert hat, aber das Paket „pcmcia“ deaktiviert hat, könnte man dennoch einen PCMCIA-Treiber in der `config/base.txt` auswählen, ohne dass eine Fehlermeldung beim Erstellen der Archive auftritt. Um das zu verhindern, kann man den regulären Ausdruck auch abhängig von einer YESNO-Variablen in der Konfiguration erweitern. Dazu wird der Name der Variablen, die bestimmt ob der Ausdruck erweitert wird, mit runden Klammern direkt hinter den Namen des Ausdrucks gehängt. Ist die Variable aktiv und hat den Wert „yes“, wird der Ausdruck erweitert, sonst nicht.

```
PCMCIA_NET_DRV   = 'pcnet_cs|xirc2ps_cs|3c574_cs|...' : ''
+NET_DRV(OPT_PCMCIA) = '(RE:PCMCIA_NET_DRV)' : ''
```



Wird jetzt `OPT_PCMCIA='no'` gesetzt, und in der `config/base.txt` wird z. B. der PCMCIA-Treiber `xirc2ps_cs` benutzt, gibt es beim Erstellen der Archive eine Fehlermeldung.

**Hinweis:** Dies funktioniert *nicht*, wenn die Variable nicht explizit in der Konfigurationsdatei gesetzt wird, sondern ihren Wert über eine Standard-Belegung in der `check/<PAKET>.txt` erhält. In diesem Fall muss man also in der Konfigurationsdatei die Variable explizit setzen und ggf. auf die Standard-Belegung verzichten.

### Regulären Ausdruck in Abhängigkeit von anderen Variablen erweitern

Alternativ kann man auch beliebige Werte von Variablen als Bedingung verwenden, die Syntax sieht dann wie folgt aus:

```
+NET_DRV(KERNEL_VERSION=~'^3\.18\..*$') = ...
```

Wenn `KERNEL_VERSION` zu dem angegebenen regulären Ausdruck passt, also irgendein Kernel aus der 3.18er Versionsreihe genutzt wird, dann wird die Liste der erlaubten Netzwerktreiber um die angegebenen Treiber ergänzt.

**Hinweis:** Dies funktioniert *nicht*, wenn die Variable nicht explizit in der Konfigurationsdatei gesetzt wird, sondern ihren Wert über eine Standard-Belegung in der `check/<PAKET>.txt` erhält. In diesem Fall muss man also in der Konfigurationsdatei die Variable explizit setzen und ggf. auf die Standard-Belegung verzichten.

### Fehlermeldungen

Findet die Prüfung einen Fehler, erscheint eine Fehlermeldung der folgenden Art:

```
Error: wrong value of variable HOSTNAME: '' (may not be empty)
Error: wrong value of variable MOUNT_OPT: 'rx' (user supplied regular expression)
```

Beim ersten Fehler wurde der Ausdruck in einer `check/<PAKET>.exp`-Datei definiert und ein Hinweis auf den Fehler wird mit ausgegeben. Im zweiten Falle wurde der Ausdruck direkt in einer `check/<PAKET>.txt`-Datei spezifiziert, deshalb gibt es keinen zusätzlichen Hinweis auf die Fehlerursache.

### Definition regulärer Ausdrücke

Reguläre Ausdrücke sind wie folgt definiert:

Regulärer Ausdruck: Eine oder mehrere Alternativen, getrennt durch '|', z. B. „ro|rw|no“. Trifft eine der Alternativen zu, trifft der ganze Ausdruck zu (hier wären „ro“, „rw“ und „no“ gültige Ausdrücke).

Eine Alternative ist eine Verkettung mehrerer Teilstücke, die einfach aneinandergereiht werden.

Ein Teilstück ist ein „Atom“, gefolgt von einem einzelnen „\*“, „+“, „?“ oder „{min, max}“. Die Bedeutung ist wie folgt:

- „a\*“ — beliebig viele „a“s (erlaubt auch den Fall, das gar kein „a“ da ist)
- „a+“ — mindestens ein „a“
- „a?“ — kein oder ein „a“

- „a{2,5}“ — zwei bis fünf „a“s
- „a{5}“ — genau fünf „a“s
- „a{2,}“ — mindestens zwei „a“s
- „a{,5}“ — höchstens fünf „a“s

Ein „Atom“ ist ein

- regulärer Ausdruck eingeschlossen in Klammern, z. B. trifft „(a|b)+“ auf eine beliebige Zeichenkette zu, die mindestens ein „a“ oder „b“ enthält, sonst aber beliebig viele und in beliebiger Reihenfolge
- ein leeres Paar Klammern steht für einen „leeren“ Ausdruck
- ein Ausdruck mit eckigen Klammern „[]“ (siehe weiter unten)
- ein Punkt „.“, der auf irgendein einzelnes Zeichen zutrifft, z. B. trifft „.+“ auf eine beliebige Zeichenkette zu, die mindestens ein Zeichen enthält
- ein „^“ steht für den Zeilenanfang, z. B. trifft „^a.\*“ auf eine Zeichenkette zu, die mit einem „a“ anfängt und in der beliebige Zeichen folgen, etwa „a“ oder „adkadhashdkash“
- ein „\$“ steht für das Zeilenende
- ein „\“ gefolgt von einem der Sonderzeichen `^ . [ $ ( ) | * + ? { \` steht für genau das zweite Zeichen ohne seine spezielle Bedeutung
- ein normales Zeichen trifft auf genau das Zeichen zu, z. B. trifft „a“ genau auf „a“ zu.

Ein Ausdruck in rechteckigen Klammern bedeutet Folgendes:

- „x-y“ — trifft auf irgendein Zeichen zu, das zwischen „x“ und „y“ liegt, z. B. steht „[0-9]“ für alle Zeichen zwischen „0“ und „9“; „[a-zA-Z]“ steht für alle Buchstaben, egal ob groß oder klein
- „^ x-y“ — trifft auf irgendein Zeichen zu, das *nicht* im angegebenen Intervall liegt; so steht z. B. „[^ 0-9]“ für alle Zeichen, die *keine* Ziffern sind
- „[:character-class:]“ — trifft auf ein Zeichen der Zeichenklasse *character-class* zu. Relevante Standardzeichenklassen sind: `alnum`, `alpha`, `blank`, `digit`, `lower`, `print`, `punct`, `space`, `upper` und `xdigit`. So steht „[:alpha:]“ für alle Groß- und Kleinbuchstaben und ist somit identisch zu „[:lower:] [:upper:]“.

### Beispiele für reguläre Ausdrücke

Sehen wir uns das mal an einigen Beispielen an!

**NUMERIC:** Ein numerischer Wert besteht aus mindestens einer, aber ansonsten beliebig vielen Ziffern. „Mindestens ein“ drückt man mit „+“ aus, eine Ziffer hatten wir schon als Beispiel. Zusammengesetzt ergibt das:

```
NUMERIC = '[0-9]+'
```

oder alternativ

```
NUMERIC = '[:digit:]*'
```

NOBLANK: Ein Wert, der keine Leerzeichen enthält, ist ein beliebiges Zeichen (außer dem Leerzeichen) und davon beliebig viele:

```
NOBLANK = '[^ ]*'
```

bzw. wenn der Wert zusätzlich auch nicht leer sein darf:

```
NOBLANK = '[^ ]+'
```

IPADDR: Sehen wir uns das Ganze nochmal am Beispiel der IPv4-Adresse an. Eine IPv4-Adresse besteht aus vier „Octets“, die durch einen Punkt („.“) voneinander getrennt sind. Ein Octet kann eine Zahl zwischen 0 und 255 sein. Definieren wir als erstes ein Octet. Es kann

eine Zahl zwischen 0 und 9 sein:	[0-9]
eine Zahl zwischen 10 und 99:	[1-9][0-9]
eine Zahl zwischen 100 und 199:	1[0-9][0-9]
eine Zahl zwischen 200 und 249:	2[0-4][0-9]
eine Zahl zwischen 250 und 255 sein:	25[0-5]

Das Ganze sind Alternativen, also fassen wir sie einfach mittels „|“ zu einem Ausdruck zusammen: „[0-9]|[1-9][0-9]|1[0-9][0-9]|2[0-4][0-9]|25[0-5]“ und haben damit ein Octet. Daraus können wir nun eine IPv4-Adresse machen, vier Octets mit Punkten voneinander getrennt (der Punkt muss mittels eines *Backslashes* maskiert werden, da er sonst für ein beliebiges Zeichen steht). Basierend auf der Syntax der exp-Dateien sieht das Ganze dann wie folgt aus:

```
OCTET  = '[0-9]|[1-9][0-9]|1[0-9][0-9]|2[0-4][0-9]|25[0-5] '
IPADDR = '(\(RE:OCTET\)\\.){3}(RE:OCTET)'
```

### Unterstützung beim Entwurf regulärer Ausdrücke

Will man reguläre Ausdrücke entwerfen und testen, kann man dazu das „regex“-Programm verwenden, das sich in dem Verzeichnis **unix** bzw. **windows** des Pakets „base“ befindet. Es akzeptiert die folgende Syntax:

```
usage: regex [-c <check dir>] <regex> <string>
```

Dabei bedeuten die Parameter Folgendes:

- **<check dir>** ist das Verzeichnis, das die Check-Dateien und damit auch die exp-Dateien enthält. Diese werden von „regex“ eingelesen, damit man auf bereits definierte Ausdrücke zurückgreifen kann.
- **<regex>** ist der reguläre Ausdruck (im Zweifelsfall immer in '...' oder "... " angeben, wobei doppelte Anführungsstriche nur nötig sind, wenn einfache Hochkommata in dem Ausdruck vorkommen sollen)
- **<string>** ist die zu prüfende Zeichenkette

Das könnte z. B. wie folgt aussehen:

```
./i586-linux-regex -c ../check '[0-9]' 0
adding user defined regular expression='[0-9]' ('^([0-9])$')
checking '0' against regexp '[0-9]' ('^([0-9])$')
'[0-9]' matches '0'

./i586-linux-regex -c ../check '[0-9]' a
adding user defined regular expression='[0-9]' ('^([0-9])$')
checking 'a' against regexp '[0-9]' ('^([0-9])$')
regex error 1 (No match) for value 'a' and regexp '[0-9]' ('^([0-9])$')

./i586-linux-regex -c ../check IPADDR 192.168.0.1
using predefined regular expression from base.exp
adding IPADDR='((RE:OCTET)\.){3}(RE:OCTET)'
('^(((1?[0-9]?[0-9]|2[0-4][0-9]|25[0-5])\.){3}(1?[0-9]?[0-9]|2[0-4][0-9]|25[0-5]))$')
'IPADDR' matches '192.168.0.1'

./i586-linux-regex -c ../check IPADDR 192.168.0.256
using predefined regular expression from base.exp
adding IPADDR='((RE:OCTET)\.){3}(RE:OCTET)'
('^(((1?[0-9]?[0-9]|2[0-4][0-9]|25[0-5])\.){3}(1?[0-9]?[0-9]|2[0-4][0-9]|25[0-5]))$')
regex error 1 (No match) for value '192.168.0.256' and regexp
'((RE:OCTET)\.){3}(RE:OCTET)'
(unknown:-1) wrong value of variable cmd_var: '192.168.0.256' (invalid ipv4 address)
```

### 8.3.7. Erweiterte Prüfungen der Konfiguration

Manchmal ist es notwendig, komplexere Überprüfungen durchzuführen. Beispiele für solche komplexeren Dinge wären z. B. Abhängigkeiten zwischen Paketen oder Bedingungen, die nur erfüllt sein müssen, wenn Variablen bestimmte Werte annehmen. So muss z. B. bei Auswahl eines PCMCIA-ISDN-Adapters auch das Paket „pcmcia“ installiert werden.

Um diese Überprüfungen durchführen zu können, kann man in `check/<PAKET>.ext` (auch ext-Skript genannt) kleinere Tests schreiben. Die Sprache besteht aus folgenden Elementen:

#### 1. Schlüsselwörter:

- Kontrollfluss:
  - if (*expr*) then *statement* else *statement* fi
  - foreach *var* in *set\_var* do *statement* done
  - foreach *var* in *set\_var\_1* ... *set\_var\_n* do *statement* done
  - foreach *var* in *var\_n* do *statement* done
- Abhängigkeiten:
  - provides *package* version *x.y.z*
  - depends on *package* version *x1.y1 x2.y2.z2 x3.y3* ...
- Aktionen:
  - warning "*warning*"
  - error "*error*"

```

- fatal_error "fatal error"
- set var = value
- crypt (variable)
- stat (filename, res)
- fgrep (filename, regex)
- split (string, set_variable, character)

```

2. Datentypen: Zeichenketten, positive ganze Zahlen, Versionsnummern

3. Logische Operationen: <, ==, >, !=, !, &&, ||, =~, copy\_pending, samenet, subnet

## Datentypen

Zu den Datentypen ist zu sagen, dass Variablen auf Grund des zugehörigen regulären Ausdrucks fest einem Datentyp zugeordnet werden:

- Variablen, deren Typ mit „NUM“ beginnt, sind numerisch und enthalten positive ganze Zahlen
- Variablen, die eine N-Variable für irgendein Array sind, sind ebenfalls numerisch
- alle anderen Variablen werden wie Zeichenketten verarbeitet

Das bedeutet unter anderem, dass eine Variable vom Typ `ENUMERIC` *nicht* als Index beim Zugriff auf eine Array-Variable benutzt werden kann, auch wenn man sich vorher vergewissert hat, dass sie nicht leer ist. Der folgende Code funktioniert somit nicht:

```

# sei TEST eine Variable vom Typ ENUMERIC
if (test != "")
then
    # Fehler: You can't use a non-numeric ID in a numeric
    #         context. Check type of operand.
    set i=my_array[test]
    # Fehler: You can't use a non-numeric ID in a numeric
    #         context. Check type of operand.
    set j=test+2
fi

```

Eine Lösung für dieses Problem bietet [split](#) (Seite 365):

```

if (test != "")
then
    # alle Elemente von test_% sind numerisch
    split(test, test_%, ' ', numeric)
    # OK
    set i=my_array[test_%[1]]
    # OK
    set j=test_%[1]+2
fi

```

## Zeichenketten und Variablenersetzung

An verschiedenen Stellen werden Zeichenketten benötigt, etwa wenn eine [Warnung](#) (Seite 360) ausgegeben werden soll. In einigen Fällen, die in dieser Dokumentation beschrieben werden, wird eine solche Zeichenkette dabei nach Variablen durchsucht; werden welche gefunden, werden diese durch ihren Inhalt oder andere Attribute *ersetzt*. Diese Ersetzung wird *Variablenersetzung* genannt.

Dies soll an einem Beispiel verdeutlicht werden. Es gelte die Konfiguration:

```
# config/base.txt
HOSTNAME='fli41'
# config/dns_dhcp.txt
HOST_N='1' # Anzahl der Hosts
HOST_1_NAME='client'
HOST_1_IP4='192.168.1.1'
```

Dann werden die Zeichenketten wie folgt umgeschrieben, wenn die Variablenersetzung in dem jeweiligen Kontext aktiv ist:

```
"Mein Router heißt $HOSTNAME"
# --> "Mein Router heißt fli41"
"HOSTNAME ist Teil des Pakets ${HOSTNAME}"
# --> "HOSTNAME ist Teil des Pakets base"
"@HOST_N ist $HOST_N"
# --> " # Anzahl der Hosts ist 1"
```

Wie man sehen kann, gibt es prinzipiell drei Möglichkeiten der Ersetzung:

- **\$<Name>** bzw. **\${<Name>}**: Ersetzt den Variablennamen durch den Inhalt der Variable. Dies ist die häufigste Form der Ersetzung. Der Name muss in `{...}` stehen, wenn direkt danach in der Zeichenkette ein Zeichen kommt, das gültiger Bestandteil eines Variablennamens sein kann, also ein Buchstabe, eine Ziffer oder ein Unterstrich. In allen anderen Fällen ist die Verwendung von geschweiften Klammern möglich, aber nicht zwingend.
- **%<Name>** bzw. **%\${<Name>}**: Ersetzt den Variablennamen durch den Namen des Pakets, in dem die Variable definiert ist. Dies funktioniert *nicht* bei im Skript via [set](#) (Seite 360) zugewiesenen Variablen oder bei Laufvariablen einer [foreach-Schleife](#) (Seite 367), da solche Variablen kein Paket besitzen und für Laufvariablen diese Syntax eine andere Bedeutung erhält.
- **@<Name>** bzw. **@\${<Name>}**: Ersetzt den Variablennamen durch den Kommentar, der in der Konfiguration hinter der Variablen steht. Auch dies ergibt keinen Sinn für im Skript definierte Variablen.

Will man ein „\$“, „@“ oder „%“ im Text haben, schreibt man „\$\$“, „@@“ bzw. „%%“.

**Hinweis:** Elemente von Array-Variablen können auf diese Weise *nicht* in Zeichenketten integriert werden, weil es keine Möglichkeit gibt, einen Index anzugeben.

Generell unterliegen nur *Konstanten* der Variablenersetzung; Zeichenketten, die über eine Variable hereinkommen, bleiben unverändert. Ein Beispiel soll dies verdeutlichen - es sei die folgende Konfiguration gegeben:

```
HOSTNAME='fli41'
TEST='${HOSTNAME}'
```

Dann führt der Code:

```
warning "${TEST}"
```

zur Ausgabe von:

```
Warning: ${HOSTNAME}
```

und *nicht* zur Ausgabe von:

```
Warning: fli41
```

In den folgenden Abschnitten wird explizit darauf hingewiesen, unter welchen Umständen Zeichenketten der Variablenersetzung unterliegen.

### Definition eines Dienstes mit einer dazugehörenden Versionsnummer: **provides**

Damit kann z. B. ein OPT deklarieren, dass es einen Drucker-Dienst oder einen Webserver-Dienst bereitstellt. Es kann jeweils nur ein einziges Paket geben, dass einen Dienst bereitstellt. Damit kann man verhindern, dass z. B. zwei Webserver parallel installiert werden, was nahe-liegenderweise nicht gehen würde, da sich die beiden Server um den Port 80 streiten würden. Zusätzlich wird die aktuelle Version des Dienstes angegeben, so dass Weiterentwicklungen Rechnung getragen werden kann. Die Versionsnummer besteht aus zwei- oder drei Zahlen, die durch Punkte voneinander getrennt sind, etwa „4.0“ oder „2.1.23“.

Typischerweise werden Dienste auf OPTs, nicht auf ganze Pakete abgebildet. So besitzt etwa das Paket „tools“ eine ganze Reihe von Programmen, die jeweils ihre eigene **provides**-Anweisung definieren, so sie denn via `OPT_...='yes'` aktiviert sind.

Die Syntax lautet:

```
provides <Name> version <Version>
```

Beispiel aus dem Paket „easycron“:

```
provides cron version 3.10.0
```

Die Versionsnummer sollte vom OPT-Entwickler in der dritten Komponente angehoben werden, wenn lediglich Funktionserweiterungen vorgenommen wurden und die Schnittstelle zum OPT kompatibel geblieben ist. Die Versionsnummer sollte in der ersten oder zweiten Komponente angehoben werden, wenn sich die Schnittstelle in irgendeiner Weise inkompatibel verändert hat (z. B. auf Grund von Variablenumbenennungen, Pfad-Änderungen, verschwundenen oder umbenannten Dienstprogrammen etc.).

**Definition einer Abhängigkeit zu einem Dienst mit einer bestimmten Version: depends**

Benötigt man zur Erbringung der eigenen Funktionalität einen anderen Dienst (z. B. einen Webserver), kann man hiermit diese Abhängigkeit zu einem Dienst mit einer bestimmten Version spezifizieren. Die Version kann zweistellig (z. B. „2.1“) oder dreistellig (z. B. „2.1.11“) angegeben werden, wobei die zweistellige Variante alle Versionen akzeptiert, die ebenfalls so beginnen, während die dreistellige Version nur genau diese angegebene Version akzeptiert. Des Weiteren kann eine Liste von solchen Versionsnummern angegeben werden, falls mehrere Versionen des Dienstes kompatibel mit dem Paket sind.

Die Syntax lautet:

```
depends on <Name> version <Version>+
```

Ein Beispiel: Paket „server“ enthalte:

```
provides server version 1.0.1
```

Sei ein Paket „client“ gegeben. Darin seien folgende `depends`-Anweisungen beispielhaft enthalten:<sup>5</sup>

```
depends on server version 1.0      # OK, '1.0' passt zu '1.0.1'
depends on server version 1.0.1    # OK, '1.0.1' passt zu '1.0.1'
depends on server version 1.0.2    # Fehler, '1.0.2' passt nicht zu '1.0.1'
depends on server version 1.1      # Fehler, '1.1' passt nicht zu '1.0.1'
depends on server version 1.0 1.1  # OK, '1.0' passt zu '1.0.1'
depends on server version 1.0.2 1.1 # Fehler, weder '1.0.2' noch '1.1' passen
                                   # zu '1.0.1'
```

**Kommunikation mit dem Nutzer: warning, error, fatal\_error**

Mit Hilfe dieser drei Funktionen kann man Nutzer warnen, einen Fehler signalisieren oder die Prüfung sofort abbrechen. Die Syntax sieht wie folgt aus:

- `warning "text"`
- `error "text"`
- `fatal_error "text"`

Alle an diese Funktionen übergebenen Zeichenketten-Konstanten unterliegen der [Variablenersetzung](#) (Seite 358).

**Zuweisungen**

Benötigt man aus irgendeinem Grund eine temporäre Variable, kann man diese einfach mit „`set var [= value]`“ anlegen. *Die Variable darf kein Konfigurationsvariable sein!*<sup>6</sup> Lässt man den „`= value`“ Teil weg, wird die Variable einfach auf „yes“ gesetzt, so dass man sie hinterher einfach in einer `if`-Anweisung testen kann. Wird ein Zuweisungsteil angegeben, kann hinter

<sup>5</sup>Natürlich nur jeweils eine zur selben Zeit!

<sup>6</sup>Dies ist eine bewusste Entscheidung: Durch `check`-Skripte lässt sich die Benutzerkonfiguration *nicht* verändern.



dem Gleichheitszeichen alles stehen: normale Variablen, indizierte Variablen, Zahlen, Zeichenketten, Versionsnummern.

Zu beachten ist, dass durch diese Zuweisung gleichzeitig der *Typ* der temporären Variablen festgelegt wird. Wird eine Zahl zugewiesen, „merkt“ mkfli41 sich, dass diese Variable eine Zahl enthält, und erlaubt später das Rechnen damit. Versucht man, mit einer anders getypten Variable zu rechnen, wird dies fehlschlagen. Beispiel:

```
set i=1    # OK, i ist eine numerische Variable
set j=i+1  # OK, j ist eine numerische Variable und enthält den Wert 2
set i="1"  # OK, i ist nun eine Zeichenketten-Variable
set j=i+1  # Fehler "You can't use a non-numeric ID in a numeric
           #          context. Check type of operand."
           # --> mit Zeichenketten kann man nicht rechnen!
```

Man kann auch temporäre Arrays (siehe unten) anlegen. Beispiel:

```
set prim_%[1]=2
set prim_%[2]=3
set prim_%[3]=5
warning "${prim_n}"
```

Dabei wird die Anzahl der Elemente in dem Array in der Variable `prim_n` von mkfli41 verwaltet. Der obige Code führt somit zu folgender Ausgabe:

```
Warning: 3
```

Wenn auf der rechten Seite einer Zuweisung eine Zeichenketten-Konstante steht, unterliegt sie zum Zeitpunkt der Zuweisung der [Variablenersetzung](#) (Seite 358). Dies wird im folgenden Beispiel demonstriert. Der Code:

```
set s="a"
set v1="$s" # v1="a"
set s="b"
set v2="$s" # v2="b"
if (v1 == v2)
then
  warning "gleich"
else
  warning "ungleich"
fi
```

produziert die Ausgabe „ungleich“, weil die Variablen `v1` und `v2` bereits während der Zuweisung den aktuellen Inhalt der Variablen `s` ersetzen.

**Hinweis:** Eine in einem Skript gesetzte Variable ist bei der Abarbeitung weiterer Skripte sichtbar – es existiert zur Zeit kein Lokalisierungsprinzip für derart eingeführte Variablen. Da die Reihenfolge, in der die Skripte verschiedener Pakete abgearbeitet wird, nicht definiert ist, sollte man sich nie darauf verlassen, dass Variablen irgendwelche Werte besitzen bzw. von einem anderen Paket übernommen haben.

## Arrays

Will man auf einzelne Elemente einer %-Variablen (eines Arrays) zugreifen, muss man den Original-Namen der Variable, wie er in der `check/<PAKET>.txt`-Datei steht, verwenden, und dabei für jedes „%-Zeichen einen Index mit Hilfe von „*Index*“ anhängen.

Beispiel: Will man auf die Elemente der Variable `PF_USR_CHAIN_%_RULE_%` zugreifen, benötigt man zwei Indizes, weil die Variable zwei „%-Zeichen besitzt. Alle Elemente ausgeben kann man z. B. mit Hilfe des folgenden Codes (die `foreach`-Schleife wird [weiter unten](#) (Seite 367) erläutert):

```
foreach i in pf_usr_chain_n
do
    # nur ein Index nötig, da nur ein '%' im Variablennamen
    set j_n=pf_usr_chain_%_rule_n[i]
    # Achtung: ein
    # foreach j in pf_usr_chain_%_rule_n[i]
    # ist leider nicht möglich, deshalb der Umweg über j_n!
    foreach j in j_n
    do
        # zwei Indizes nötig, da zwei '%' im Variablennamen
        set rule=pf_usr_chain_%_rule_%[i][j]
        warning "Rule $i/$j: ${rule}"
    done
done
```

Mit der folgenden Beispiel-Konfiguration

```
PF_USR_CHAIN_N='2'
PF_USR_CHAIN_1_NAME='usr-chain_a'
PF_USR_CHAIN_1_RULE_N='2'
PF_USR_CHAIN_1_RULE_1='ACCEPT'
PF_USR_CHAIN_1_RULE_2='REJECT'
PF_USR_CHAIN_2_NAME='usr-chain_b'
PF_USR_CHAIN_2_RULE_N='1'
PF_USR_CHAIN_2_RULE_1='DROP'
```

gibt es dann die folgenden Ausgaben:

```
Warning: Rule 1/1: ACCEPT
Warning: Rule 1/2: REJECT
Warning: Rule 2/1: DROP
```

Alternativ kann man direkt über alle Werte des Arrays iterieren, kennt dann allerdings nicht die exakten Indizes der Einträge (was auch nicht immer erforderlich ist):

```
foreach rule in pf_usr_chain_%_rule_%
do
    warning "Rule %{rule}='${rule}'"
done
```

Das produziert mit der Beispiel-Konfiguration von oben die folgenden Ausgaben:

```
Warning: Rule PF_USR_CHAIN_1_RULE_1='ACCEPT'
Warning: Rule PF_USR_CHAIN_1_RULE_2='REJECT'
Warning: Rule PF_USR_CHAIN_2_RULE_1='DROP'
```

An dem zweiten Beispiel sieht man auch schön die Bedeutung der %<Name>-Syntax: Innerhalb der Zeichenkette wird %rule durch den *Namen* der betrachteten Variable ersetzt (also z. B. PF\_USR\_CHAIN\_1\_RULE\_1), während \$rule durch dessen *Inhalt* (also z. B. ACCEPT) ersetzt wird.

### Verschlüsseln eines Passwortes: crypt

Einige Variablen enthalten Passwörter, die nicht im Klartext in der rc.cfg stehen sollen. Diese Variablen können mittels **crypt** verschlüsselt werden und werden damit in das Format überführt, dass auch auf dem Router benötigt wird. Verwendet wird das wie folgt:

```
crypt (<Variable>)
```

Die crypt-Funktion ist die *einzige* Stelle, an der eine Konfigurationsvariable verändert werden kann.

### Abfragen von Eigenschaften einer Datei: stat

stat ermöglicht es, Eigenschaften einer Datei abzufragen. Zur Verfügung gestellt wird im Augenblick lediglich die Größe einer Datei. Wenn man auf Dateien unterhalb des aktuellen Konfigurationsverzeichnis testen will, kann man die interne Variable config\_dir benutzen. Die Syntax lautet:

```
stat (<Dateiname>, <Schlüssel>)
```

Der Aufruf sieht wie folgt aus (wobei die verwendeten Parameter nur Beispiele sind):

```
foreach i in openvpn_%_secret
do
    stat("${config_dir}/etc/openvpn/$i.secret", keyfile)
    if (keyfile_res != "OK")
    then
        error "OpenVPN: missing secretfile <config>/etc/openvpn/$i.secret"
    fi
done
```

In dem Beispiel wird geprüft, ob eine Datei im aktuellen Konfigurationsverzeichnis vorhanden ist. Wenn also OPENVPN\_1\_SECRET='test' in der Konfigurationsdatei gesetzt wird, prüft die Schleife im ersten Durchlauf, ob im aktuellen Konfigurationsverzeichnis die Datei etc/openvpn/test.secret vorhanden ist.

Nach dem Aufruf sind zwei Variablen definiert:

- <Schlüssel>\_res: Resultat des Systemaufrufs stat() („OK“, wenn Systemruf erfolgreich, sonst Fehlermeldung des Systemaufrufs)
- <Schlüssel>\_size: Größe der Datei

Das könnte dann z. B. so aussehen:

```

stat ("unix/Makefile", test)
if ("$test_res" == "OK")
then
    warning "test_size = $test_size"
else
    error "Error '$test_res' while trying to get size of 'unix/Makefile'"
fi

```

Ein als Zeichenketten-Konstante übergebener Dateiname unterliegt der [Variablenersetzung](#) (Seite 358).

### Durchsuchen von Dateien: **fgrep**

Wenn Sie in einer Datei per „grep“<sup>7</sup> suchen wollen, steht Ihnen das **fgrep**-Kommando zur Verfügung. Die Syntax lautet:

```
fgrep (<Dateiname>, <RegEx>)
```

Wenn die Datei <Dateiname> nicht existiert wird **mkfli41** mit einem fatalen Fehler beendet! Wenn Sie also nicht sicher sind, ob die Datei immer vorhanden ist, testen Sie die Existenz von <Dateiname> vorher mit **stat** ab. Nach dem Aufruf von **fgrep** steht Ihnen das Suchresultat in dem Array **FGREP\_MATCH\_%** zur Verfügung, wobei der Index *x* wie üblich von eins bis **FGREP\_MATCH\_N** reicht. **FGREP\_MATCH\_1** verweist dabei auf den gesamten Bereich der Zeile, auf den der reguläre Ausdruck gepasst hat, während **FGREP\_MATCH\_2** bis **FGREP\_MATCH\_N** den jeweils *n-1*-ten geklammerten Teil beinhalten.

Ein erstes einfaches Beispiel soll die Verwendung demonstrieren. Die Datei **opt/etc/shells** enthält die Zeile:

```
/bin/sh
```

Der folgende Code

```

fgrep("opt/etc/shells", "~/(.)(.*)/")
foreach v in FGREP_MATCH_%
do
    warning "%v='$v'"
done

```

produziert die folgende Ausgabe:

```

Warning: FGREP_MATCH_1='/bin/'
Warning: FGREP_MATCH_2='b'
Warning: FGREP_MATCH_3='in'

```

Der reguläre Ausdruck hat (nur) auf „/bin/“ gepasst, deshalb steht auch (nur) dieser Teil der Zeile in der Variable **FGREP\_MATCH\_1**. Der erste geklammerte Teil im Ausdruck passt auf das erste Zeichen hinter dem ersten „/“, deshalb steht auch nur „b“ in **FGREP\_MATCH\_2**. Der zweite geklammerte Teil umfasst den Rest hinter den „b“ bis zum letzten „/“, somit steht „in“ in der Variable **FGREP\_MATCH\_3**.

Das folgende zweite Beispiel demonstriert eine praxisnahe Verwendung von **fgrep** an einem Beispiel aus der **check/base.ext**. Hier wird getestet, ob alle in der **PF\_FORWARD\_x** angegebenen **tmpl:-**Referenzen vorhanden sind:

---

<sup>7</sup> „grep“ ist ein auf Unix-Betriebssystemen verbreitetes Kommando zum Filtern von Textströmen.

```

foreach n in pf_forward_n
do
  set rule=pf_forward_%[n]
  if (rule =~ "tpl:([[:space:]]+)")
  then
    foreach m in match_%
    do
      stat("$config_dir/etc/fwrules.tpl/$m", tplfile)
      if(tplfile_res == "OK")
      then
        add_to_opt "etc/fwrules.tpl/$m"
      else
        stat("opt/etc/fwrules.tpl/$m", tplfile)
        if(tplfile_res == "OK")
        then
          add_to_opt "etc/fwrules.tpl/$m"
        else
          fgrep("opt/etc/fwrules.tpl/templates", "^$m[[:space:]]+")
          if (fgrep_match_n == 0)
          then
            error "Can't find tpl:$m for PF_FORWARD_${n}='$rule'!"
          fi
        fi
      fi
    done
  fi
done

```

Sowohl ein als Zeichenketten-Konstante übergebener Dateiname als auch als Zeichenketten-Konstante übergebener regulärer Ausdruck unterliegen der [Variablenersetzung](#) (Seite 358).

### Auseinandernehmen von Parametern: `split`

Oftmals werden Variablen mit mehreren Parametern belegt, die dann in Startup-Skripten erst wieder auseinandergenommen werden. Will man diese bereits vorher auseinandernehmen und Tests auf ihnen durchführen, nimmt man `split`. Die Syntax lautet:

```
split (<Zeichenkette>, <Array>, <Trennzeichen>)
```

Die Zeichenkette kann durch eine Variable oder direkt als Konstante angegeben werden. `mkfli4l` zerlegt ihn an den Stellen, an denen das Trennzeichen auftaucht, und erzeugt pro Teil ein Element des Arrays. Über diese Elemente kann man dann hinterher iterieren und Prüfungen vornehmen. Steht zwischen zwei Trennzeichen nichts, wird ein Array-Element mit einer leeren Zeichenkette als Wert erzeugt. Ausnahme ist „`:`“: Hier werden alle Leerzeichen konsumiert und keine leeren Variablen erzeugt.

Sollen die bei der Zerlegung entstandenen Elemente in einem numerischen Kontext verwendet werden (z.B. als Indizes), muss das beim Aufruf von `split` spezifiziert werden. Das geschieht durch das zusätzliche Attribut „`numeric`“. Der Aufruf sieht dann wie folgt aus:

```
split (<Zeichenkette>, <Array>, <Trennzeichen>, numeric)
```

Ein Beispiel:

```

set bar="1.2.3.4"
split (bar, tmp_%, '.', numeric)
foreach i in tmp_%
do
    warning "%i = $i"
done

```

Die produzierte Ausgabe ist:

```

Warning: TMP_1 = 1
Warning: TMP_2 = 2
Warning: TMP_3 = 3
Warning: TMP_4 = 4

```

**Hinweis:** Wenn die „numeric“-Variante verwendet wird, dann prüft `mkfli4l` zum Zeitpunkt der Zerlegung *nicht*, ob die Teil-Zeichenketten auch wirklich numerisch sind! Bei einer späteren Verwendung in einem numerischen Kontext (etwa beim Addieren) löst `mkfli4l` jedoch einen fatalen Fehler aus, wenn eine solche Variable doch nicht numerisch ist. Beispiel:

```

set bar="a.b.c.d"
split (bar, tmp_%, '.', numeric)
# Fehler: invalid number 'a'
set i=tmp_%[1]+1

```

Eine an `split` im ersten Parameter übergebene Zeichenketten-Konstante unterliegt der [Variablenersetzung](#) (Seite 358).

### Hinzufügen von Dateien zum Archiv: `add_to_opt`

Mit der Funktion `add_to_opt` können zusätzliche Dateien ans `opt`- oder `rootfs`-Archiv angehängt werden. Es können dabei *alle* Dateien unterhalb von `opt/` oder aus dem Konfigurationsverzeichnis ausgewählt werden. Eine Beschränkung nur auf die Dateien, die mit einem bestimmten Paket geliefert werden, gibt es nicht. Liegt eine Datei sowohl unter `opt/` als auch im Konfigurationsverzeichnis im gleichen Pfad, bevorzugt `add_to_opt` die Dateien aus dem Konfigurationsverzeichnis. Die Funktion `add_to_opt` wird in der Regel dann eingesetzt, wenn komplexe logische Regeln darüber entscheiden, ob und welche Dateien in das Archiv aufgenommen werden müssen.

Die Syntax sieht wie folgt aus:

```
add_to_opt <Datei> [<Flags>]
```

Die Flags sind optional. Es gelten die in Tabelle 8.2 aufgeführten Standard-Werte, falls keine Flags angegeben sind.

Es folgt ein Beispiel aus dem Paket „sshd“:

```

if (opt_sshd)
then
    foreach pkf in sshd_public_keyfile_%
    do
        stat("$config_dir/etc/ssh/$pkf", publickeyfile)
        if(publickeyfile_res == "OK")

```

```

then
    add_to_opt "etc/ssh/$pkf" "mode=400 flags=utxt"
else
    error "sshd: missing public keyfile %pkf=$pkf"
fi
done
fi

```

Mit **stat** (Seite 363) wird zunächst geprüft, ob die Datei im Konfigurationsverzeichnis existiert. Ist die Datei vorhanden, wird sie ans Archiv angehängt, andernfalls bricht **mkfli4l** mit einer entsprechenden Fehlermeldung ab.

**Hinweis:** Auch bei **add\_to\_opt** **prüft** (Seite 347) **mkfli4l** zuerst, ob die zu kopierende Datei im Konfigurationsverzeichnis zu finden ist.

Sowohl ein als Zeichenketten-Konstante übergebener Dateiname als auch als Zeichenketten-Konstante übergebene Flags unterliegen der **Variablenersetzung** (Seite 358).

### Kontrollfluss

```

if (expr)
then
    statement
else
    statement
fi

```

Eine klassische Fallunterscheidung, wie man sie kennt. Ist die Bedingung wahr, wird der **then**-Teil ausgeführt, ist die Bedingung falsch, wird der **else**-Teil ausgeführt.

Will man Tests über Array-Variablen durchführen, muss man jede einzelne Variable testen. Dazu gibt es die **foreach**-Schleife in zwei Varianten.

1. Iterieren über Array-Variablen:

```

foreach <Laufvariable> in <Array-Variable>
do
    <Anweisung>
done

foreach <Laufvariable> in <Array-Variable-1> <Array-Variable-2> ...
do
    <Anweisung>
done

```

Diese Schleife iteriert über alle angegebenen Array-Variablen, jeweils angefangen beim ersten Element bis hin zum letzten; die Anzahl der Elemente im Array wird dabei der dem Array zugeordneten N-Variable entnommen. Die Laufvariable nimmt dabei die jeweiligen Werte der Array-Variablen an. Zu beachten ist dabei, dass bei optionalen Array-Variablen, die in der Konfiguration nicht vorhanden sind, ein leeres Element generiert wird. Unter Umständen muss das im Skript berücksichtigt werden, was man z.B. wie folgt tun kann:

```

foreach i in template_var_opt_%
do
    if (i != "")
    then
        warning "%i is present (%i='$i')"
    else
        warning "%i is undefined (empty)"
    fi
done

```

Wie man auch am Beispiel erkennen kann, lässt sich der *Name* der jeweiligen Array-Variablen durch die %<Laufvariable>-Konstruktion ermitteln.

Die Anweisung in der Schleife kann eine der oben beschriebenen Kontrollelemente oder Funktionen (`if`, `foreach`, `provides`, `depends`, ...) sein.

Will man auf genau ein Element eines Arrays zugreifen, kann man dieses mittels der Syntax <Array>[<Index>] ansprechen. Der Index kann dabei eine normale Variable, eine Zahlenkonstante oder wiederum ein indiziertes Array sein.

## 2. Iterieren über N-Variablen:

```

foreach <Laufvariable> in <N-Variable>
do
    <Anweisung>
done

```

Diese Schleife läuft von 1 bis zum Wert, der in der N-Variable steht. Man kann die Laufvariable dazu benutzen, um Array-Variablen zu indizieren. Will man also nicht nur über eine Array-Variable iterieren, sondern über mehrere gleichzeitig, die alle durch *dieselben* N-Variable kontrolliert werden, nimmt man diese Variante der Schleife und verwendet die Laufvariable zum Indizieren mehrerer Array-Variablen. Beispiel:

```

foreach i in host_n
do
    set name=host_%_name[i]
    set ip4=host_%_ip4[i]
    warning "$i: name=$name ip4=$ip4"
done

```

Das ergibt bei entsprechend gefüllten HOST\_%\_NAME- und HOST\_%\_IP4-Arrays beispielsweise:

```

Warning: 1: name=berry ip4=192.168.11.226
Warning: 2: name=fence ip4=192.168.11.254
Warning: 3: name=sandbox ip4=192.168.12.254

```

## Ausdrücke

Ausdrücke verknüpfen Werte und Operatoren zu einem neuen Wert. Ein Wert kann dabei eine gewöhnliche Variable, ein Array-Element oder eine Konstante (Zahl, Zeichenkette oder Versionsnummer) sein. Alle Zeichenketten-Konstanten, die in Ausdrücken auftreten, unterliegen der [Variablenersetzung](#) (Seite 358).



Operatoren erlauben so gut wie alles, was man von einer Programmiersprache gewöhnt ist. Ein Test auf die Gleichheit zweier Variablen könnte also so aussehen:

```
var1 == var2
"$var1" == "$var2"
```

Zu beachten ist dabei, dass der Vergleich in Abhängigkeit vom Typ der Variable erfolgt, der in `check/<PAKET>.txt` festgelegt wurde. Ist eine der beiden Variablen **numerisch** (Seite 357), erfolgt der Vergleich auf numerischer Basis, d. h. die Zeichenketten werden in Zahlen umgewandelt und dann verglichen. Sonst erfolgt der Vergleich auf Zeichenketten-Basis; ein Vergleich `"05" == "5"` ergibt „falsch“, ein Vergleich `"18" < "9"` ergibt „wahr“ auf Grund der lexikographischen Ordnung auf Zeichenketten: die Ziffer „1“ liegt vor der Ziffer „9“ im zugrunde liegenden ASCII-Zeichensatz.

Für den Vergleich von Versionen wird das Hilfskonstrukt `numeric(version)` eingeführt, welches den numerischen Wert für eine Versionsnummer für Vergleichszwecke bestimmt. Dabei gilt:

```
numeric(version) := major * 10000 + minor * 1000 + sub
```

wobei „major“ die erste Komponente der Versionsnummer darstellt, „minor“ die zweite und „sub“ die dritte; fehlt „sub“, entfällt der Term in der obigen Summe einfach (oder anders ausgedrückt, für „sub“ wird null angenommen).

Eine vollständige Auflistung aller Ausdrücke ist in Tabelle 8.3 zu finden. Dabei steht „val“ für einen beliebig getypten Wert, „number“ für einen numerischen Wert und „string“ für eine Zeichenkette.

Tabelle 8.3.: Logische Ausdrücke

Ausdruck	wahr wenn
<code>id</code>	<code>id == „yes“</code>
<code>val == val</code>	identisch getypte Werte sind gleich
<code>val != val</code>	identisch getypte Werte sind ungleich
<code>val == number</code>	numerischer Wert von <code>val == number</code>
<code>val != number</code>	numerischer Wert von <code>val != number</code>
<code>val &lt; number</code>	numerischer Wert von <code>val &lt; number</code>
<code>val &gt; number</code>	numerischer Wert von <code>val &gt; number</code>
<code>val == version</code>	<code>numeric(val) == numeric(version)</code>
<code>val &lt; version</code>	<code>numeric(val) &lt; numeric(version)</code>
<code>val &gt; version</code>	<code>numeric(val) &gt; numeric(version)</code>
<code>val =~ string</code>	regulärer Ausdruck in <code>string</code> auf <code>val</code> passt
<code>( expr )</code>	Ausdruck in Klammern ist wahr
<code>expr &amp;&amp; expr</code>	beide Ausdrücke sind wahr
<code>expr    expr</code>	mind. einer der beiden Audrücke ist wahr
<code>copy_pending(id)</code>	siehe Beschreibung
<code>samenet (string1, string2)</code>	<code>string1</code> das gleiche netz wie <code>string2</code> beschreibt
<code>subnet (string1, string2)</code>	<code>string1</code> ein Subnetz von <code>string2</code> beschreibt

## Match-Operator

Mit dem Match-Operator `=~` kann man prüfen, ob ein regulärer Ausdruck auf den Wert einer Variable passt. Weiterhin kann man den Operator auch nutzen, um Teilausdrücke aus einer Variablen zu extrahieren. Nach erfolgreichem Anwenden eines regulären Ausdrucks auf eine Variable enthält das Array `MATCH_%` die gefundenen Teile. Das könnte z. B. wie folgt aussehen:

```
set foo="foobar12"
if ( foo =~ "(foo)(bar)([0-9]*)" )
then
    foreach i in match_%
    do
        warning "match %i: $i"
    done
fi
```

Ein `mkfli4l`-Aufruf führt dann zu folgender Ausgabe:

```
Warning: match MATCH_1: foo
Warning: match MATCH_2: bar
Warning: match MATCH_3: 12
```

Bei Verwendung von `=~` kann Bezug auf alle existierenden regulären Ausdrücke genommen werden. Will man z. B. prüfen, ob ein PCMCIA-Ethernet-Treiber ausgewählt wurde, ohne dass `OPT_PCMCIA` auf „yes“ gesetzt wurde, könnte das wie folgt aussehen:

```
if (!opt_pcmcia)
then
    foreach i in net_drv_%
    do
        if (i =~ "(RE:PCMCIA_NET_DRV)$")
        then
            error "If you want to use ..."
        fi
    done
fi
```

Wie in dem Beispiel demonstriert wird, ist es wichtig, den regulären Ausdruck mit Hilfe von `^` und `$` zu *verankern*, wenn man den Ausdruck auf die *gesamte* Variable anwenden will. Ansonsten liefert der Match-Ausdruck schon „wahr“, wenn nur ein *Teil* der Variable vom regulären Ausdruck abgedeckt wird, was in diesem Fall sicherlich nicht erwünscht ist.

## Prüfen, ob in Abhängigkeit vom Wert einer Variable eine Datei kopiert wurde:

### `copy_pending`

Mit den im Check-Prozess gewonnenen Informationen prüft die Funktion `copy_pending`, ob in Abhängigkeit vom Wert einer Variable eine Datei kopiert wurde oder nicht. Das kann man verwenden, um z. B. zu testen, ob der vom Nutzer angegebene Treiber auch wirklich existiert und kopiert wurde. `copy_pending` akzeptiert den zu prüfenden Namen in Form einer Variablen oder einer Zeichenkette.<sup>8</sup> `copy_pending` prüft dazu, ob

<sup>8</sup>Wie eingangs beschrieben unterliegt die Zeichenkette der Variablenersetzung, so dass man z. B. mittels einer [foreach-Schleife](#) (Seite 367) und der [%<Name>-Ersetzung](#) (Seite 358) alle Elemente eines Arrays prüfen kann.

- die Variable aktiv ist (wenn sie von einem OPT abhängt, muss dieses auf „yes“ gesetzt sein),
- die Variable in einer `opt/<PAKET>.txt`-Datei referenziert wurde, und
- ob in Abhängigkeit vom aktuellen Wert eine Datei kopiert wurde.

Dabei liefert `copy_pending` „wahr“ zurück, wenn im letzten Schritt festgestellt wurde, dass *keine* Datei kopiert wurde, das Kopieren also somit noch aussteht (also „pending“ ist).

Ein kleines Beispiel für die Anwendung all dieser Funktionen findet man in `check/base.ext`:

```
foreach i in net_drv_%
do
    if (copy_pending("%i"))
    then
        error "No network driver found for %i='$i', check config/base.txt"
    fi
done
```

Hier werden alle Elemente des Arrays `NET_DRV_%` angemackert, für die keine Kopieraktion vorgenommen wurde, für die also in der `opt/base.txt` kein entsprechender Eintrag existiert.

### Vergleich von Netzwerkadressen: `samenet` und `subnet`

Zum Prüfen von Routen benötigt man ab und zu einen Test, ob zwei Netzwerke identisch sind oder eines ein Subnetz eines anderen ist. Dazu gibt es die beiden Funktionen `samenet` und `subnet`. Dabei liefert

```
samenet (netz1, netz2)
```

„wahr“, wenn beide Netze identisch sind, und

```
subnet (netz1, netz2)
```

gibt „wahr“ zurück, wenn „netz1“ ein Subnetz von „netz2“ ist.

### Erweitern der Kernel-Kommandozeile

Ist ein OPT gezwungen, dem Kernel andere Boot-Parameter zu übergeben, so musste früher die Variable `KERNEL_BOOT_OPTION` geprüft werden, ob der nötige Parameter enthalten war, und ggf. eine Warnung oder eine Fehlermeldung ausgegeben werden. Mit der internen Variable `KERNEL_BOOT_OPTION_EXT` kann man nötige, aber fehlende Optionen direkt im ext-Skript ergänzen. Ein Beispiel aus der `check/base.ext`:

```
if (powermanagement =~ "apm.*|none")
then
    if ( ! kernel_boot_option =~ "acpi=off")
    then
        set kernel_boot_option_ext="${kernel_boot_option_ext} acpi=off"
    fi
fi
```

Damit wird „acpi=off“ an den Kernel übergeben, falls keine Energieverwaltung oder welche vom Typ „APM“ gewünscht ist.

### 8.3.8. Unterstützung verschiedener Kernelversionslinien

Verschiedene Kernelversionslinien unterscheiden sich häufig in einigen Details:

- es stehen andere Treiber zur Verfügung, einige sind weggefallen, andere hinzugekommen
- die Module heißen teilweise einfach anders
- die Modul-Abhängigkeiten sehen anders aus
- die Module liegen woanders

Diese Unterschiede werden zum großen Teil durch `mkfli4l` automatisch behandelt. Um die zur Verfügung stehenden Module zu beschreiben, kann man zum einen die zur Prüfung verwendeten Prüfungen in Abhängigkeit von der Version erweitern ([bedingte reguläre Ausdrücke](#) (Seite 353)), und zum anderen erlaubt `mkfli4l` *versionsabhängige* `opt/<PAKET>.txt`-Dateien. Dies heißen dann `opt/<PAKET>_<Kernel-Version>.txt`, wobei die Komponenten der Kernel-Version durch Unterstriche voneinander getrennt werden. Ein Beispiel: Das Paket „base“ enthält die folgenden Dateien im `opt`-Verzeichnis:

- `base.txt`
- `base_3_18.txt`
- `base_3_19.txt`

Die erste Datei (`base.txt`) wird *immer* verarbeitet. Die anderen beiden Dateien werden nur verarbeitet, wenn die Kernelversion „3.18(.)“ bzw. „3.19(.)“ lautet. Wie man sieht, können Versionskomponenten im Dateinamen weggelassen werden, wenn man eine ganze Gruppe von Kernen „erschlagen“ möchte. Unter Annahme von `KERNEL_VERSION='3.18.9'` werden für ein Paket `<PAKET>` die folgenden Dateien (sofern vorhanden) eingelesen und verarbeitet:

- `<PAKET>.txt`
- `<PAKET>_3.txt`
- `<PAKET>_3_18.txt`
- `<PAKET>_3_18_9.txt`

### 8.3.9. Dokumentation

Die Dokumentation wird in den Dateien

- `doc/<SPRACHE>/opt/<PAKET>.txt`
- `doc/<SPRACHE>/opt/<PAKET>.html`

abgelegt. Die HTML-Dateien können auch aufgeteilt werden, d. h. für jedes enthaltene OPT eine. Dann muss trotzdem eine `<PAKET>.html` angelegt werden, die auf die anderen Dateien verweist. Änderungen sollten in folgenden Dateien dokumentiert werden:

- `changes/<PAKET>.txt`

Die gesamte Text-Dokumentation darf keine Tabulatoren enthalten und muss nach spätestens 79 Zeichen einen harten Zeilenumbruch haben. Die stellt sicher, dass die Dokumentation auch mit einem Editor ohne automatischen Zeilenumbruch richtig gelesen werden kann.

Wer mag kann auch eine Dokumentation im  $\text{\LaTeX}$ -Format erstellen und daraus dann HTML- und PDF-Fassungen erzeugen. Als Beispiel kann die Dokumentation von fli4l dienen. Einen Rahmen für die Dokumentation und die minimal benötigten  $\text{\LaTeX}$ -Macros kann man im Paket „template“ finden. Eine kurze Beschreibung ist in den folgenden Unterabschnitten zu finden.

Die fli4l-Dokumentation steht zur Zeit in den folgenden Sprachen zur Verfügung: deutsch, englisch ( $\langle\text{SPRACHE}\rangle = \text{„english“}$ ) und französisch ( $\langle\text{SPRACHE}\rangle = \text{„french“}$ ). Es steht einem Paket-Entwickler jedoch frei, sein Paket in beliebigen Sprachen zu dokumentieren. Im Sinne der Verständlichkeit wird jedoch empfohlen, eine Dokumentation in deutsch und/oder englisch (idealerweise in beiden Sprachen) anzufertigen.

### Voraussetzungen für die Erstellung einer $\text{\LaTeX}$ -Dokumentation

Zum Erstellen der Dokumentation aus  $\text{\LaTeX}$ -Quellen gibt es folgende Anforderungen an die Umgebung:

- Linux/OS X-Umgebung: Zur einfachen Erzeugung gibt es ein Makefile, mit dem alle weiteren Aufrufe automatisiert sind (Cygwin müsste auch funktionieren, wird aber nicht vom fli4l-Team getestet)
- LaTeX2HTML für die HTML-Version
- natürlich  $\text{\LaTeX}$  (empfohlen wird „TeX Live“ für Linux/OS X und „MiKTeX“ für Microsoft Windows) mit dem „pdfTeX“-Programm und folgenden  $\text{\TeX}$ -Paketen:
  - aktuelles KOMA-Skript (mindestens Version 2)
  - alle notwendigen Pakete für pdfTeX
  - ausgepacktes Dokumentationspaket für fli4l, welches die benötigten Makefiles und  $\text{\TeX}$ -Stile bereitstellt

### Dateinamen

Die Dateien der Dokumentation werden nach folgendem Schema benannt:

**$\langle\text{PAKET}\rangle\_main.tex$ :** Diese Datei enthält den Hauptteil der Dokumentation.  $\langle\text{PAKET}\rangle$  steht hier für den Namen des Pakets, das beschrieben werden soll (in Kleinbuchstaben).

**$\langle\text{PAKET}\rangle\_appendix.tex$ :** Sollen zu diesem Paket noch weitere Anmerkungen im Anhang hinzugefügt werden, so werden diese hier abgelegt.

Diese Dateien werden im Verzeichnis `fli4l/ $\langle\text{PAKET}\rangle$ /doc/ $\langle\text{SPRACHE}\rangle$ /tex/ $\langle\text{PAKET}\rangle$`  abgelegt. Für das Paket „sshd“ sieht das z. B. wie folgt aus:

```
$ ls fli4l/doc/deutsch/tex/sshd/
Makefile sshd_appendix.tex  sshd_main.tex  sshd.tex
```

Das Makefile ist für die Generierung der Dokumentation verantwortlich, die `sshd.tex`-Datei stellt einen Rahmen für die eigentliche Dokumentation und den Anhang bereit, der sich in den anderen beiden Dateien befindet. Ansehen kann man sich das am Beispiel der Dokumentation des „template“-Pakets.

## LaTeX-Grundlagen

LaTeX arbeitet ähnlich wie HTML „Tag-orientiert“, nur dass die Tags hier „Kommandos“ heißen und folgendes Format aufweisen: `\kommando` bzw. `\begin{umgebung} ... \end{umgebung}`

Nach Möglichkeit sollte man mit Hilfe von Kommandos eher die *Bedeutung* des jeweiligen Textes auszeichnen und weniger dessen *Darstellung*. Es ist also vorteilhaft, z. B.

```
\warning{Bitte nicht ... tun}
statt
\emph{Bitte nicht ... tun}
zu verwenden.
```

Jedes Kommando bzw. jede Umgebung kann noch weitere Parameter aufnehmen, die mit `\kommando{parameter1}{parameter2}{parameterN}` geschrieben werden.

Manche Kommandos haben optionale Parameter, die in eckigen (statt geschweiften) Klammern stehen: `\kommando[optionalerParameter]{parameter1} ...`. Dabei kommt im Normalfall nur ein optionaler Parameter vor, in seltenen Fällen aber auch mehrere.

Einzelne Absätze werden im Dokument durch Leerzeilen getrennt. Innerhalb dieser Absätze nimmt LaTeX selbst den Zeilenumbruch und die Worttrennung vor.

Folgende Buchstaben haben eine spezielle Bedeutung in LaTeX und müssen, sollten sie in normalem Text vorkommen, mit einem vorangestellten `\` maskiert werden: `# $ & _ % { }`. „~“ und „^“ müssen wie folgt geschrieben werden: `\verb?~? \verb?^?`

Die wichtigsten LaTeX-Kommandos werden in der Dokumentation des „template“-Pakets verwendet und erklärt.

### 8.3.10. Dateiformate

Alle Textdateien (sowohl Dokumentation als auch Skripte, die später auf dem Router liegen) müssen im DOS-Dateiformat, also mit CR/LF statt nur LF am Zeilenende in das Paket gelegt werden. Dadurch wird erreicht, dass Windows-Nutzer die Dokumentation auch mit „notepad“ lesen können und durch eine Änderung eines Skripts unter Windows das Ganze später auf dem Router trotzdem lauffähig bleibt. Die Skripte werden beim Bauen der Archive in das auf dem Router benötigte Format konvertiert (siehe die Beschreibung der Flags in Tabelle 8.2).

### 8.3.11. Entwickler-Dokumentation

Sollte ein Programm aus dem Paket eine neue Schnittstelle definieren, die andere Programme nutzen können, so ist die Dokumentation dieser Schnittstelle in einer separaten Dokumentation unter `doc/dev/<PAKET>.txt` abzulegen.

### 8.3.12. Client-Programme

Sollte ein Paket zusätzliche Client-Programme mitliefern, so sind diese im Verzeichnis `windows/` für Windows-Clients und im Verzeichnis `unix/` für Unix- und Linux-Clients abzulegen.

### 8.3.13. Quellcode

Angepasste Programme und Quellcodes können im Verzeichnis `src/<PAKET>/` beigelegt werden. Sollen die Programme genauso wie die restlichen fli4l-Programme gebaut werden, bitte einen Blick in die Dokumentation des „src“-Pakets (Seite 293) werfen.

### 8.3.14. Weitere Dateien

Alle Dateien, die nachher auf dem Router liegen, werden unter `opt/` abgelegt. Dabei liegen unter:

- `opt/etc/boot.d/` und `opt/etc/rc.d/` Skripte, die beim Starten des Systems ausgeführt werden sollen
- `opt/etc/rc0.d/` Skripte, die beim Herunterfahren des Systems ausgeführt werden
- `opt/etc/ppp/` Skripte, die beim Einwählen und Auflegen ausgeführt werden
- `opt/` die ausführbaren Programme und sonstige Dateien entsprechend ihrer Positionen im Dateisystem (d. h. die Datei `opt/bin/busybox` wird später auf dem Router im Verzeichnis `/bin` liegen)

Die Skripte in `opt/etc/boot.d/`, `opt/etc/rc.d/` und `opt/etc/rc0.d/` werden wie folgt benannt:

```
rc<nummer>.<name>
```

Die Nummer entscheidet über die Reihenfolge der Ausführung, der Name gibt einen Hinweis darauf, welches Programm/Paket von diesem Skript behandelt wird.

## 8.4. Allgemeine Skript-Erstellung auf fli4l

Hier folgt jetzt *keine* allgemeine Einführung in Shell-Skripte, das kann jeder im Internet selber nachlesen, es wird nur auf die spezielle Gegebenheiten bei fli4l eingegangen. Informationen dazu gibt es in den diversen Unix-/Linux-Hilfeseiten. Folgende Links können als Einstiegspunkte zu diesem Thema dienen:

- Einführung in Shell-Skripte:
  - <http://cip.physik.uni-freiburg.de/main/howtos/sh.php>
- Hilfeseiten online:
  - <http://linux.die.net/>
  - <http://heapsort.de/man2web>
  - <http://man.he.net/>
  - [http://www.linuxcommand.org/superman\\_pages.php](http://www.linuxcommand.org/superman_pages.php)

### 8.4.1. Aufbau

In der Unix-Welt ist es nötig, ein Skript mit dem Namen des Interpreters zu beginnen, daher steht in der ersten Zeile:

```
#!/bin/sh
```

Damit man später leichter erkennen kann, was ein Skript macht und wer es geschrieben hat, sollte jetzt ein kurzer Header folgen, in etwa so:

```
#-----
# /etc/rc.d/rc500.dummy - start my cool dummy server
#
# Creation:      19.07.2001  Toller Hecht <toller-hecht@example.net>
# Last Update:   11.11.2001  Süße Maus <suesse-maus@example.net>
#-----
```

Nun kann das eigentliche Skript folgen...

#### 8.4.2. Umgang mit Konfigurationsvariablen

Pakete werden über die Datei `config/<PACKAGE>.txt` konfiguriert. Die darin enthaltenen und [aktiven Variablen](#) (Seite 348) werden beim Erzeugen des Boot-Mediums in die Datei `rc.cfg` übernommen. Beim Booten des Routers wird diese Datei eingelesen, bevor irgend ein rc-Skript (Skripte unter `/etc/rc.d/`) gestartet wird. Diese Skripte können dadurch auf alle Konfigurationsvariablen einfach durch `$<Variablenname>` zugreifen.

Benötigt man Werte von Konfigurationsvariablen auch noch nach dem Booten, dann kann man sie aus der `/etc/rc.cfg` extrahieren, in welche während des Bootens die Konfiguration des Boot-Mediums geschrieben wurde. Möchte man beispielsweise den Wert der Variable `OPT_DNS` in einem Skript auslesen, so kann man dies folgendermaßen tun:

```
eval $(grep "^OPT_DNS=" /etc/rc.cfg)
```

Das funktioniert auch mit mehreren Variablen effizient (d. h. mit nur einem Aufruf des `grep`-Programms):

```
eval $(grep "^\(HOSTNAME\|DOMAIN_NAME\|OPT_DNS\|DNS_LISTEN_N\)=" /etc/rc.cfg)
```

#### 8.4.3. Persistente Speicherung von Daten

Gelegentlich benötigt ein Paket die Möglichkeit, Daten persistent abzulegen, die also einen Neustart des Routers überleben. Dazu existiert die Funktion `map2persistent`, die von einem Skript in `/etc/rc.d/` aufgerufen werden kann. Sie erwartet eine Variable, die einen Pfad enthält, und ein Unterverzeichnis. Die Idee ist, dass die Variable entweder einen tatsächlichen Pfad beschreibt – dann wird dieser Pfad auch genommen, denn der Nutzer hat ihn so gewünscht, oder die Zeichenkette „auto“ – dann wird unterhalb eines Verzeichnisses auf einem persistenten Medium ein entsprechendes Unterverzeichnis gemäß dem zweiten Parameter erzeugt. Die Funktion liefert das Resultat in eben der Variable zurück, deren Name im ersten Parameter übergeben wurde.

Ein Beispiel soll dies verdeutlichen. Sei `VBOX_SPOOLPATH` eine Variable, die einen Pfad oder die Zeichenkette „auto“ enthält. Dann führt der Aufruf

```
begin_script VBOX "Configuring vbox ..."
[...]
map2persistent VBOX_SPOOLPATH /spool
[...]
end_script
```

dazu, dass die Variable `VBOX_SPOOLPATH` entweder gar nicht verändert wird (falls sie einen Pfad enthält), oder dass sie durch den Pfad `/var/lib/persistent/vbox/spool` ersetzt wird (falls sie die Zeichenkette „auto“ enthält). Dabei verweist<sup>9</sup> `/var/lib/persistent` auf ein Ver-

<sup>9</sup>mit Hilfe eines so genannten „bind“-Mounts



zeichnis auf einem beschreibbaren und nicht flüchtigen Speichermedium, und `<SCRIPT>` stellt das aufrufende Skript in Kleinbuchstaben dar (dieser Name wird vom ersten Argument des `begin_script-Aufrufs` (Seite 377) abgeleitet). Falls kein geeignetes Medium existieren sollte (was durchaus sein kann), ist `/var/lib/persistent` ein Verzeichnis in der RAM-Disk.

Zu beachten ist, dass der Pfad, der von `map2persistent` zurückgegeben wird, *nicht* automatisch erzeugt wird – das muss der Aufrufer selbst erledigen (etwa durch einen Aufruf von `mkdir -p <Pfad>`).

In der Datei `/var/run/persistent.conf` kann nachgeschaut werden, ob die persistente Speicherung von Daten möglich ist. Beispiel:

```
. /var/run/persistent.conf
case $SAVETYPE in
persistent)
    echo "Persistente Speicherung möglich!"
    ;;
transient)
    echo "Persistente Speicherung NICHT möglich!"
    ;;
esac
```

#### 8.4.4. Fehlersuche

Bei Start-Skripten ist es oft sinnvoll, diese bei Bedarf im Debug-Modus der Shell laufen zu lassen, um festzustellen, wo „der Wurm drin ist“. Dazu wird am Anfang und am Ende folgendes eingefügt:

```
begin_script <OPT-Name> "start message"
<script code>
end_script
```

Im normalen Betrieb erscheint jetzt beim Start des Skriptes der angegebene Text und am Ende der gleiche Text mit einem vorangestellten „finished“.

Will man die Skripte debuggen, muss man zwei Dinge tun:

1. Man muss `DEBUG_STARTUP` (Seite 36) auf „yes“ setzen.
2. Man muss das Debuggen für dieses OPT aktivieren. Das tut man in der Regel durch den Eintrag

```
<OPT-Name>_DO_DEBUG='yes'
```

in der Konfigurationsdatei.<sup>10</sup> Jetzt wird während der Ausführung am Bildschirm genau dargestellt, was passiert.

<sup>10</sup>Manchmal werden mehrere Start-Skripte verwendet, die dann auch verschiedene Namen für ihre Debug-Variablen haben. Hier hilft ein kurzer Blick in die Skripte.

**Weitere beim Debuggen hilfreiche Variablen**

**DEBUG\_ENABLE\_CORE** Diese Variable gestattet das Erzeugen von „Core-Dumps“ (Speicherausgüssen). Stürzt ein Programm aufgrund eines Fehlers ab, wird ein Abbild des aktuellen Zustandes im Dateisystem abgelegt, der hinterher zur Analyse des Problems verwendet werden kann. Die Core-Dumps werden unter `/var/log/dumps/` abgelegt.

**DEBUG\_IP** Wird diese Variable gesetzt, werden alle Aufrufe des Programms `ip` protokolliert.

**DEBUG\_IPUP** Wird diese Variable auf „yes“ gesetzt, werden während der Ausführung der `ip-up/ip-down`-Skripte die ausgeführten Anweisungen mitgezeichnet und im System-Protokoll gespeichert.

**LOG\_BOOT\_SEQ** Wird diese Variable auf „yes“ gesetzt, protokolliert der `bootlogd` während des Bootens alle auf der Konsole getätigten Ausgaben in der Datei `/var/tmp/boot.log`. Diese Variable hat standardmäßig den Wert „yes“.

**DEBUG\_KEEP\_BOOTLOGD** Normalerweise wird der `bootlogd` am Ende des Bootvorganges beendet. Ein Setzen dieser Variable unterbindet das und erlaubt ein Protokollieren der Konsolenausgaben über den Bootvorgang hinaus.

**DEBUG\_MDEV** Ein Setzen dieser Variable generiert ein Protokoll des `mdev`-Daemons, der für das Anlegen der Geräte-Dateien unter `/dev` zuständig ist.

**8.4.5. Hinweise**

- Es ist *immer* besser, geschweifte Klammern „`{...}`“ an Stelle von runden Klammern „`(...)`“ zu benutzen. Allerdings muss dabei darauf geachtet werden, dass nach der öffnenden Klammer ein Leerzeichen oder eine neue Zeile vor dem nächsten Befehl kommt und vor der schließenden Klammer ein Semikolon oder auch eine neue Zeile kommt. Beispielsweise ist

```
{ echo "cpu"; echo "quit"; } | ...
```

gleichbedeutend mit:

```
{
    echo "cpu"
    echo "quit"
} | ...
```

- Ein Skript kann mit „`exit`“ vorzeitig beendet werden. Dies ist aber bei den Start-Skripten (`opt/etc/boot.d/...`, `opt/etc/rc.d/...`), den Stopp-Skripten (`opt/etc/rc0.d/...`) und den `ip-up/ip-down`-Skripten (`opt/etc/ppp/...`) geradezu tödlich, da auch nachfolgende Skripte nicht mehr ausgeführt werden. Im Zweifelsfall immer weglassen.
- KISS – Keep it small and simple. Du willst Perl als Skript-Sprache verwenden? Dir reichen die Skripting-Möglichkeiten von `fi4l` nicht? Überdenke deine Einstellung! Ist dein `OPT` wirklich nötig? `fi4l` ist immer noch „nur“ ein Router, ein Router sollte eigentlich keine Serverdienste anbieten.

- Die Fehlermeldung „: not found“ heißt meistens, dass das Skript noch im DOS-Format vorliegt. Weitere Fehlerquelle: Das Skript ist nicht ausführbar. In beiden Fällen sollte die `opt/<PACKAGE>.txt`-Datei daraufhin geprüft werden, ob sie die korrekten Optionen (in Bezug auf „mode“, „gid“, „uid“ und Flags) enthält. Wenn das Skript erst beim Booten erzeugt wird, sollte ein `„chmod +x <Skriptname>“` ausgeführt werden.
- Für temporäre Dateien sollte der Pfad `/tmp` genutzt werden. Es ist aber unbedingt darauf zu achten, dass hier nur wenig Platz ist, weil dies in der RootFS-RAM-Disk liegt! Wenn mehr Platz benötigt wird, muss man sich eine eigene RAM-Disk erstellen und mounten. Details dazu verrät der Abschnitt „RAM-Disks“ in dieser Dokumentation.
- Damit temporäre Dateien eindeutige Namen erhalten, sollte man grundsätzlich die aktuelle Prozess-ID, die in der Shell-Variablen `„$“` gespeichert ist, an den Dateinamen anhängen. `/tmp/<OPT-Name>.$$` stellt somit einen guten Dateinamen dar, `/tmp/<OPT-Name>` eher weniger, wobei `<OPT-Name>` natürlich nicht so stehen bleiben soll, sondern geeignet ersetzt werden muss.

## 8.5. Arbeit mit dem Paketfilter

### 8.5.1. Hinzufügen von eigenen Ketten und Regeln

Zur Manipulation des Paketfilters steht eine Reihe von Routinen zur Verfügung, mit deren Hilfe man Ketten (engl. „Chains“) und Regeln hinzufügen und wieder löschen kann. Eine Kette ist eine benannte und geordnete Liste von Regeln. Es gibt einen Satz vordefinierter Ketten (`PREROUTING`, `INPUT`, `FORWARD`, `OUTPUT`, `POSTROUTING`); mit Hilfe dieser Funktionen können weitere Ketten nach Bedarf erstellt werden.

**add\_chain/add\_nat\_chain <chain>:** Fügt eine Kette zur „filter“- oder „nat“-Tabelle hinzu.

**flush\_chain/flush\_nat\_chain <chain>:** Entfernt alle Regeln aus einer Kette der „filter“- oder „nat“-Tabelle.

**del\_chain/del\_nat\_chain <chain>:** Entfernt eine Kette aus der „filter“- oder „nat“-Tabelle. Ketten müssen leer sein, bevor sie gelöscht werden können, und es darf auch keine Referenz mehr auf sie geben. Eine solche Referenz ist z. B. eine JUMP-Aktion, deren Ziel eben diese Kette ist.

**add\_rule/ins\_rule/del\_rule:** Fügt Regeln am Ende einer Kette (`add_rule`) bzw. an beliebiger Stelle in einer Kette (`ins_rule`) ein bzw. löscht Regeln aus einer Kette (`del_rule`). Ein Aufruf sieht wie folgt aus:

```
add_rule <table> <chain> <rule> <comment>
ins_rule <table> <chain> <rule> <position> <comment>
del_rule <table> <chain> <rule> <comment>
```

wobei die Parameter folgende Bedeutung haben:

**table** Die Tabelle, in der sich die Kette befindet

**chain** Die Kette, in welche die Regel eingefügt werden soll

**rule** Die Regel, die eingefügt werden soll; das Format entspricht dem in der Konfigurationsdatei verwendeten

**position** Die Position, an der die Regel eingefügt werden soll (nur bei `ins_rule`)

**comment** Ein Kommentar, der zusammen mit der Regel angezeigt werden soll, wenn sich jemand den Paketfilter ansieht.

### 8.5.2. Einordnen in bestehende Regeln

fi4l konfiguriert den Paketfilter mit einem gewissen Standardregelsatz. Will man eigene Regeln einfügen, wird man diese in der Regel nach dem Standardregelsatz einfügen wollen. Ebenfalls wird man wissen wollen, was denn die vom Nutzer gewünschte Aktion beim Verwerfen eines Paketes ist. Diese Informationen bekommt man für die `FORWARD`- und `INPUT`-Ketten durch Aufruf zweier Funktionen, `get_defaults` und `get_count`. Nach Aufruf von

```
get_defaults <chain>
```

erhält man die folgenden Ergebnisse:

**drop:** Diese Variable enthält die Kette, in die verzweigt wird, wenn ein Paket verworfen wird.

**reject:** Diese Variable enthält die Kette, in die verzweigt wird, wenn ein Paket abgelehnt wird.

Nach Aufruf von

```
get_count <chain>
```

erhält man in der Variable `res` die Anzahl der Regeln in der Kette `<chain>`. Diese Position ist insofern wichtig, als man *nicht* einfach `add_rule` verwenden kann, um eine Regel am Ende der vordefinierten „filter“-Ketten `INPUT`, `FORWARD` und `OUTPUT` einzufügen. Dies liegt daran, dass diese Ketten mit einer Standardregel abgeschlossen werden, welche alle verbliebenen Pakete behandelt, je nach Belegung der `PF_<Kette>_POLICY`-Variablen. Ein Einfügen *hinter* dieser letzten Regel hat also keine Auswirkungen. Die Funktion `get_count` erlaubt es nun hingegen, die Stelle direkt *vor* dieser letzten Regel zu ermitteln und die Position dann an die `ins_rule`-Funktion im Parameter `<position>` zu übergeben, um die Regel wie gewünscht am Ende der jeweiligen Kette, aber vor der letzten Auffang-Regel einzubauen.

Ein Beispiel aus dem Skript `opt/etc/rc.d/rc390.dns_dhcp` des Pakets „`dns_dhcp`“ soll dies verdeutlichen:

```
case $OPT_DHCPRELAY in
  yes)
    begin_script DHCRELAY "starting dhcprelay ..."

    idx=1
    interfaces=""
    while [ $idx -le $DHCPRELAY_IF_N ]
    do
      eval iface='$DHCPRELAY_IF_'$idx

      get_count INPUT
      ins_rule filter INPUT "prot:udp  if:$iface:any 68 67 ACCEPT" \
```

```

        $res "dhcrelay access"

        interfaces=$interfaces' -i '$iface
        idx=`expr $idx + 1`
    done
    dhcrelay $interfaces $DHCPRELAY_SERVER

    end_script
;;
esac

```

Hier sieht man inmitten der Schleife einen Aufruf von `get_count`, gefolgt von einem Aufruf der `ins_rule`-Funktion, der unter anderem die `res`-Variable als `position`-Parameter übergeben wird.

### 8.5.3. Erweiterung der Paketfilter-Tests

fi4l verwendet in den Paketfilterregeln die Syntax `match:params`, um zusätzliche Bedingungen an die Pakete zu stellen (siehe `mac:`, `limit:`, `length:`, `prot:`, ...). Will man zusätzliche Tests hinzufügen, wird das folgendermaßen gemacht:

1. Festlegen eines passenden Namens. Dieser Name muss mit einem Kleinbuchstaben im Bereich a-z beginnen und ansonsten aus beliebigen Buchstaben und Ziffern bestehen.

**Wenn der Paketfilter-Test in IPv6-Regeln verwendet werden soll, dann muss darauf geachtet werden, dass der Name keine gültige IPv6-Adresskomponente ist!**

2. Anlegen einer Datei `opt/etc/rc.d/fwrules-<name>.ext`. In dieser Datei steht in etwa Folgendes:

```

# IPv4 extension is available
foo_p=yes

# the actual IPv4 extension, adding matches to match_opt
do_foo()
{
    param=$1
    get_negation $param
    match_opt="$match_opt -m foo $neg_opt --fooval $param"
}

# IPv6 extension is available
foo6_p=yes

# the actual IPv6 extension, adding matches to match_opt
do6_foo()
{
    param=$1
    get_negation6 $param
    match_opt="$match_opt -m foo $neg_opt --fooval $param"
}

```

Der Paketfilter-Test muss nicht zwingend sowohl für IPv4 als auch für IPv6 implementiert sein (obwohl dies zu bevorzugen ist, falls er für beide Layer-3-Protokolle sinnvoll ist).

### 3. Testen der Erweiterung:

```
$ cd opt/etc/rc.d
$ sh test-rules.sh 'foo:bar ACCEPT'
add_rule filter FORWARD 'foo:bar ACCEPT'
iptables -t filter -A FORWARD -m foo --fooval bar -s 0.0.0.0/0 \
    -d 0.0.0.0/0 -m comment --comment foo:bar ACCEPT -j ACCEPT
```

### 4. Aufnahme der Erweiterung und aller noch benötigten Dateien (iptables-Komponenten) ins Archiv über einen der bekannten Mechanismen.

### 5. Zulassen der Erweiterung in der Konfiguration durch Erweitern von FW\_GENERIC\_MATCH und/oder FW\_GENERIC\_MATCH6 in einer exp-Datei, z. B. wie folgt:

```
+FW_GENERIC_MATCH(OPT_FOO) = 'foo:bar' : ''
+FW_GENERIC_MATCH6(OPT_FOO) = 'foo:bar' : ''
```

## 8.6. CGI-Erstellung für das *httpd*-Paket

### 8.6.1. Allgemeines zum Webserver

Der Webserver, der bei fli4l verwendet wird, ist der *mini\_httpd* von ACME Labs. Die Quellen können unter [http://www.acme.com/software/mini\\_httpd/](http://www.acme.com/software/mini_httpd/) heruntergeladen werden. Allerdings wurden für fli4l ein paar Änderungen vorgenommen. Die Anpassungen befinden sich im *src*-Paket im Verzeichnis *src/fbr/buildroot/package/mini\_httpd*.

### 8.6.2. Skriptnamen

Der Skriptname sollte möglichst vielsagend sein, damit er von anderen Skripten leichter zu unterscheiden ist und es keine Namensüberschneidungen bei verschiedenen OPTs gibt.

Damit die Skripte ausführbar gemacht werden und DOS-Zeilenumbrüche in Unix-Zeilenumbrüche umgewandelt werden, muss in der *opt/<PAKET>.txt* ein entsprechender Eintrag gemacht werden, siehe Tabelle 8.2 (Seite 346).

### 8.6.3. Menü-Einträge

Um einen Eintrag im Menü vorzunehmen, muss eine Eintragung in der Datei */etc/httpd/menu* vorgenommen werden. Dieser Mechanismus erlaubt es OPTs, auch im laufendem Betrieb Änderungen am Menü vorzunehmen. Dies sollte nur mit dem Skript *httpd-menu.sh* gemacht werden, da dieses darauf achtet, dass das Dateiformat dieser Datei immer konsistent ist. Um neue Menüpunkte einzufügen, wird es folgendermaßen aufgerufen:

```
httpd-menu.sh add [-p <priority>] <link> <name> [section] [realm]
```

So wird ein Eintrag mit dem Namen `<name>` in den Abschnitt `[section]` eingetragen. Wenn `[section]` weggelassen wird, wird es standardmäßig in den Abschnitt „OPT-Pakete“ eingetragen. `<link>` gibt das Ziel des neuen Links an. `<priority>` spezifiziert die Priorität eines Menüeintrags in seinem Abschnitt. Wird sie nicht angegeben, wird die Standardpriorität 500 benutzt. Die Priorität sollte eine dreistellige Nummer sein. Je kleiner die Priorität, desto weiter oben steht der Link in dem Abschnitt. Soll ein Eintrag möglichst weit nach unten, so ist z. B. die Priorität 900 zu wählen. Bei gleicher Priorität werden die Einträge nach dem Ziel des Links sortiert. Bei `[realm]` wird der Bereich angegeben, für den ein angemeldeter Benutzer mindestens die Berechtigung *view* haben muss, damit der Menüpunkt angezeigt wird. Wird `[realm]` nicht angegeben, wird der Menüpunkt immer angezeigt. Siehe hierzu auch den Abschnitt „Benutzerrechte“ (Seite 387).

Beispiel:

```
httpd-menu.sh add "neuedatei.cgi" "Hier klicken" "Tools" "tools"
```

Dieses Beispiel erzeugt im Abschnitt „Tools“ einen Link mit dem Titel „Hier klicken“ und dem Link-Ziel „neuedatei.cgi“ und legt den Abschnitt, falls dieser nicht vorhanden ist, an.

Das Skript kann auch Einträge aus dem Menü wieder entfernen:

```
httpd-menu.sh rem <link>
```

Mit diesem Aufruf wird der Eintrag mit dem Link `<link>` wieder entfernt.

**Wichtig:** Wenn mehrere Menüeinträge auf die gleiche Datei verweisen, werden alle diese Einträge aus dem Menü entfernt.

Da Abschnitte auch Prioritäten haben können, können diese auch manuell angelegt werden. Wird ein Abschnitt automatisch beim Hinzufügen eines Eintrages angelegt, erhält er automatisch die Priorität 500. Der Syntax zum Anlegen von Abschnitten lautet:

```
httpd-menu.sh addsec <priority> <name>
```

Auch hier sollte `<priority>` nur dreistellige numerische Werte annehmen.

Um sinnvolle Prioritäten in Erfahrung zu bringen, lohnt es sich, auf einem laufenden fl4l in die Datei `/etc/httpd/menu` zu schauen, die Prioritäten stehen in der zweiten Spalte.

Der Vollständigkeit halber wird hier kurz auf das Dateiformat der Menüdatei eingegangen. Wem die Funktion von `httpd-menu.sh` reicht, der kann diesen Abschnitt überspringen. Die Datei `/etc/httpd/menu` hat den folgenden Aufbau: Sie ist in vier Spalten eingeteilt. In der ersten Spalte steht ein Kennbuchstabe, der Überschriften und Einträge unterscheidet. In der zweiten Spalte steht die Sortierungspriorität. Die dritte Spalte enthält bei Einträgen das Ziel des Links und bei Überschriften einen Bindestrich, da dieses Feld bei Überschriften keine Bedeutung hat. Im Rest der Zeile steht der Text, der nachher im Menü erscheint.

Überschriften benutzen den Kennbuchstaben „t“, dann wird ein neuer Menüabschnitt begonnen. Normale Menüeinträge benutzen den Kennbuchstaben „e“. Ein Beispiel:

```
t 300 - Mein tolles OPT
e 200 meinopt.cgi Mach etwas Tolles
e 500 meinopt.cgi?mehr=ja Mach mehr Tolles
```

Beim Bearbeiten dieser Datei muss man darauf achten, dass das `httpd-menu.sh`-Skript die Datei immer sortiert abspeichert. Die einzelnen Abschnitte sind sortiert und die Einträge pro Abschnitt sind in diesem Abschnitt sortiert. Der genaue Sortieralgorithmus kann aus `httpd-menu.sh` übernommen werden – besser wäre allerdings, dieses Skript um mögliche neue Funktionen zu erweitern, damit alle Menü-Bearbeitungen an zentraler Stelle passieren.

#### 8.6.4. Aufbau eines CGI-Skriptes

##### Die Kopfzeilen

Alle Skripte des Webservers sind einfache Shell-Skripte (Interpreter wie z.B. Perl, PHP, etc. sind viel zu groß für fli4l). Sie sollten mit dem obligatorischen Skript-Header anfangen (Verweis auf den Interpreter, Name, Sinn des Skriptes, Autor, Lizenz).

##### Das Hilfsskript “cgi-helper“

Gleich nach den Kopfzeilen sollte dann schon das Hilfsskript `cgi-helper` mit folgendem Aufruf eingebunden werden:

```
. /srv/www/include/cgi-helper
```

Wichtig ist ein Leerzeichen zwischen Punkt und Schrägstrich!

Dieses Skript stellt diverse Hilfsfunktionen bereit, die das Erstellen von CGIs für fli4l wesentlich vereinfachen sollen. Außerdem werden mit dem Einbinden des `cgi-helper` auch noch Standardaufgaben ausgeführt, wie beispielsweise das Parsen von Variablen, die mit Formularen oder über die URL übergebenen wurden, oder das Laden von Sprach- und CSS-Dateien.

Tabelle 8.4 gibt einen Überblick über die Funktionen des `cgi-helper`-Skriptes.

Tabelle 8.4.: Funktionen des `cgi-helper`-Skriptes

Name	Funktion
<code>check_rights</code>	Überprüfung der Benutzerrechte
<code>http_header</code>	Ausgabe eines Standard-HTTP-Headers oder eines speziellen HTTP-Headers, beispielsweise zum Download von Dateien
<code>show_html_header</code>	Ausgabe des kompletten Seitenheaders (inkl. HTTP-Header, Kopfzeile und Menü)
<code>show_html_footer</code>	Ausgabe des Abschlusses der HTML-Seite
<code>show_tab_header</code>	Ausgabe eines Inhalt-Fensters mit Reitern
<code>show_tab_footer</code>	Ausgabe des Abschlusses des Inhaltsfensters
<code>show_error</code>	Ausgabe einer Box für Fehlermeldungen (Hintergrundfarbe: rot)
<code>show_warn</code>	Ausgabe einer Box für Warnmeldungen (Hintergrundfarbe: gelb)
<code>show_info</code>	Ausgabe einer Box für Informationen oder Erfolgsmeldungen (Hintergrundfarbe: grün)

##### Der Inhalt eines CGI-Skriptes

Um ein einheitliches Design und vor allem die Kompatibilität mit zukünftigen fli4l-Versionen zu gewährleisten, ist es sehr zu empfehlen, die Funktionen des Hilfsskriptes `cgi-helper` zu benutzen, auch wenn man in einem CGI theoretisch alle Ausgaben selbst generieren kann.

Eine einfaches CGI-Skript könnte wie folgt aussehen:



```
#!/bin/sh
# -----
# Header (c) Autor Datum
# -----
# get main helper functions
. /srv/www/include/cgi-helper

show_html_header "Mein erstes CGI"
echo '    <h2>Willkommen</h2>'
echo '    <h3>Dies ist ein Beispiel-CGI-Skript</h3>'
show_html_footer
```

### Die Funktion `show_html_header`

Die Funktion `show_html_header` erwartet eine Zeichenkette als Parameter. Diese Zeichenkette stellt den Titel der zu generierenden Seite dar. Die Funktion generiert automatisch das Menü und bindet ebenso automatisch zum Skript gehörende CSS- und Sprachdateien ein. Voraussetzung dafür ist, dass diese sich in den Verzeichnissen `/srv/www/css` bzw. `/srv/www/lang` befinden und denselben Namen (aber natürlich eine andere Endung) wie das Skript haben. Ein Beispiel:

```
/srv/www/admin/OpenVPN.cgi
/srv/www/css/OpenVPN.css
/srv/www/lang/OpenVPN.de
```

Sowohl das Benutzen von Sprachdateien als auch von CSS-Dateien ist optional. Immer eingebunden werden `css/main.css` und `lang/main.<lang>`, wobei `<lang>` der gewählten Sprache entspricht.

Der Funktion `show_html_header` können aber neben dem Titel noch weitere Parameter übergeben werden. Ein Aufruf mit allen möglichen Parametern könnte so aussehen:

```
show_html_header "Titel" "refresh=$time;url=$url;cssfile=$cssfile;showmenu=no"
```

Alle zusätzlichen Parameter müssen, wie im Beispiel gezeigt, mit Anführungszeichen umschlossen und durch ein Semikolon getrennt werden. Eine Überprüfung der Syntax erfolgt *nicht*! Es ist also notwendig, sehr genau auf die Parameterübergabe zu achten.

Hier eine kurze Übersicht über die Funktion der Parameter:

- `refresh=time`: Zeit in Sekunden in der die Seite vom Browser neu geladen werden soll
- `url=url`: die URL, die bei einem Refresh neu geladen wird
- `cssfile=cssfile`: Name einer CSS-Datei, wenn diese vom Namen des CGIs abweicht
- `showmenu=no`: unterdrückt die Anzeige des Menüs und des Headers

Sonstige Richtlinien zum Inhalt:

- Fasst euch kurz :-)
- Schreibt sauberes HTML (SelfHTML<sup>11</sup> ist da ein guter Ansatzpunkt).
- Verzichtet auf hochmodernen Schnick-Schnack (JavaScript ist i. O., wenn es nicht stört, sondern den Benutzer unterstützt, das Ganze muss auch ohne JavaScript funktionieren).

<sup>11</sup>siehe <http://de.selfhtml.org/>

**Die Funktion `show_html_footer`**

Die Funktion `show_html_footer` schließt den Block im CGI-Skript ab, der durch die Funktion `show_html_header` eingeleitet wurde.

**Die Funktion `show_tab_header`**

Damit der Inhalt eurer mit Hilfe des CGIs erzeugten Webseite auch hübsch geordnet aussieht, könnt ihr die `cgi-helper`-Funktion `show_tab_header` nutzen. Sie erzeugt dann anklickbare Reiter („Tabs“ genannt), so dass ihr eure Seite in mehrere logisch voneinander getrennte Bereiche unterteilen könnt.

Der `show_tab_header`-Funktion werden Parameter immer in Paaren übergeben. Der erste Wert entspricht dem Titel eines Reiters, der zweite dem Link. Wird als Link die Zeichenkette „no“ übergeben, wird lediglich der Titel ausgegeben und der Reiter ist nicht anklickbar (und blau).

Im folgenden Beispiel wird ein „Fenster“ mit dem Titel „Ein tolles Fenster“ erzeugt. Im Fenster steht „foo bar“:

```
show_tab_header "Ein tolles Fenster" "no"
echo "foo"
echo "bar"
show_tab_footer
```

Im nächsten Beispiel werden zwei anklickbare Reiter generiert, die dem Skript die Variable `action` mit verschiedenen Werten übergibt.

```
show_tab_header "1. Auswahltab" "$myname?action=machdies" \
                "2. Auswahltab" "$myname?action=machjenes"
echo "foo"
echo "bar"
show_tab_footer
```

Nun kann das Skript den Inhalt der Variablen `FORM_action` (siehe weiter unten zur Variablenauswertung) auswerten und je nachdem unterschiedliche Inhalte bereitstellen. Damit der angeklickte Reiter auch ausgewählt erscheint und nicht mehr angeklickt werden kann, müsste der Funktion statt dem Link wie schon erwähnt ein „no“ übergeben werden. Das geht aber auch einfacher, wenn man sich an die Konvention in folgendem Beispiel hält:

```
_opt_machdies="1. Auswahltab"
_opt_machjenes="2. Auswahltab"
show_tab_header "$_opt_machdies" "$myname?action=opt_machdies" \
                "$_opt_machjenes" "$myname?action=opt_machjenes"
case $FORM_action in
    opt_machdies) echo "foo" ;;
    opt_machjenes) echo "bar" ;;
esac
show_tab_footer
```

Wird also für den Titel eine Variable verwendet, deren Namen dem Inhalt der Variablen `action` mit führendem Unterstrich (`_`) entspricht, wird der entsprechende Reiter ausgewählt dargestellt.

### Die Funktion `show_tab_footer`

Die Funktion `show_tab_footer` schließt den Block im CGI-Skript ab, der durch die Funktion `show_tab_header` eingeleitet wurde.

### Mehrsprachfähigkeit

Das Hilfsskript `cgi-helper` enthält weiterhin Funktionen, um CGI-Skripte mehrsprachig zu machen. Dazu müssen „nur“ für alle Textausgaben Variablen mit führenden Unterstrichen (`_`) verwendet und diese Variablen in den entsprechenden Sprachdateien definiert werden.

Beispiel:

`lang/opt.de` enthalte:

```
_opt_machdies="Eine Ausgabe"
```

`lang/opt.en` enthalte:

```
_opt_machdies="An Output"
```

`admin/opt.cgi` enthalte:

```
...  
echo $_opt_machdies  
...
```

### Formular-Auswertung

Um Formulare zu verarbeiten, muss man noch einige Dinge wissen. Egal ob die Formular-Methode GET oder POST verwendet wird, die Parameter finden sich nach dem Einbinden des `cgi-helper`-Skripts (welches wiederum das Hilfsprogramm `proccgi` aufruft) in den Variablen `FORM_<Parameter>` wieder. Wenn das Formularfeld also den Namen „eingabe“ hatte, kann im CGI-Skript mit `$FORM_eingabe` darauf zugegriffen werden.

Weitere Informationen zum Programm `proccgi` finden sich unter <http://www.fpx.de/fp/Software/ProcCGI.html>.

### Benutzerrechte: Die Funktion `check_rights`

Um zu prüfen, ob der Benutzer ausreichende Rechte zur Nutzung eines CGI-Skripts besitzt, muss am Anfang des CGI-Skripts die Funktion `check_rights` wie folgt aufgerufen werden:

```
check_rights <Bereich> <Aktion>
```

Das CGI-Skript wird dann nur ausgeführt, wenn der aktuell angemeldete Benutzer

- alle Rechte hat (`HTTPD_RIGHTS_x='all'`), oder
- alle Rechte für den angegebenen Bereich hat (`HTTPD_RIGHTS_x='<Bereich>:all'`), oder
- das Recht hat, die angegebene Aktion im angegebenen Bereich auszuführen (`HTTPD_RIGHTS_x='<Bereich>:<Aktion>'`).

### Die Funktion `show_error`

Diese Funktion gibt eine Fehlermeldung in einer roten Box aus. Sie erwartet zwei Parameter: einen Titel sowie eine Meldung. Beispiel:

```
show_error "Error: No key" "No key was specified!"
```

### Die Funktion `show_warn`

Diese Funktion gibt eine Warnmeldung in einer gelben Box aus. Sie erwartet zwei Parameter: einen Titel sowie eine Meldung. Beispiel:

```
show_info "Warnung" "Derzeit besteht keine Verbindung!"
```

### Die Funktion `show_info`

Diese Funktion gibt eine Informations- oder Erfolgsmeldung in einer grünen Box aus. Sie erwartet zwei Parameter: einen Titel sowie eine Meldung. Beispiel:

```
show_info "Info" "Aktion wurde erfolgreich ausgeführt!"
```

### Das Hilfsskript “`cgi-helper-ip4`”

Gleich nach dem Hilfsskript “`cgi-helper`” kann dann das Hilfsskript `cgi-helper-ip4` mit folgendem Aufruf eingebunden werden:

```
. /srv/www/include/cgi-helper-ip4
```

Wichtig ist ein Leerzeichen zwischen Punkt und Schrägstrich!

Dieses Skript stellt Hilfsfunktionen bereit, um Prüfungen von IPv4-Adressen vornehmen zu können.

### Die Funktion `ip4_isvalidaddr`

Diese Funktion überprüft, ob eine gültige IPv4-Adresse übergeben wurde. Beispiel:

```
if ip4_isvalidaddr ${FORM_inputip}
then
    ...
fi
```

### Die Funktion `ipv4_normalize`

Diese Funktion entfernt aus der übergebenen IPv4-Adresse führende Nullen. Beispiel:

```
ip4_normalize ${FORM_inputip}
IP=$res
if [ -n "$IP" ]
then
    ...
fi
```

**Die Funktion `ipv4_isindhcprange`**

Diese Funktion prüft, ob die übergebene IPv4-Adresse sich im Bereich der übergebenen Start- und Zieladresse befindet. Beispiel:

```
if ipv4_isindhcprange $FORM_inputip $ip_start $ip_end
then
    ...
fi
```

**8.6.5. Sonstiges**

Dies und das (ja, das ist auch noch wichtig!):

- Der `mini_httpd` schützt Unterverzeichnisse nicht mit einem Passwort. Es muss für jedes Verzeichnis eine eigene `.htaccess`-Datei oder ein Link auf eine andere `.htaccess`-Datei angelegt werden.
- KISS - Keep it simple, stupid!
- Diese Angaben können sich jederzeit ohne Vorankündigung ändern!

**8.6.6. Fehlersuche**

Um die Fehlersuche innerhalb eines CGI-Skripts zu erleichtern, kann man vor der Einbindung des `cgi-helper`-Skripts den Debugging-Modus aktivieren. Dazu muss die Variable `set_debug` auf den Wert „yes“ gesetzt werden. Dies führt zur Erstellung der Datei `debug.log`, die über die URL `http://<fli4l-Host>/admin/debug.log` heruntergeladen werden kann. Diese enthält alle Aufrufe des CGIs. Die `set_debug`-Variable ist nicht global, muss also in jedem Problem-CGI erneut gesetzt werden. Beispiel:

```
set_debug="yes"
. /srv/www/include/cgi-helper
```

Alternativ kann auch die jeweilige CGI-URL um den Parameter `debug=yes` ergänzt werden, etwa `http://<fli4l-Host>/admin/meinopt.cgi?debug=yes`.

Des Weiteren eignet sich `cURL`<sup>12</sup> hervorragend zur Fehlersuche, insbesondere wenn die HTTP-Kopfzeilen nicht korrekt zusammengesetzt werden oder der Browser nur weiße Seiten anzeigt. Auch ist das Cachingverhalten moderner Webbrowser bei der Fehlersuche hinderlich.

Beispiel: Mit dem folgenden Aufruf wird der HTTP-Header („dump“, `-D`) sowie die normale Ausgabe des CGIs `admin/mein.cgi` ausgegeben. Es soll der Benutzername („user“, `-u`) „admin“ verwendet werden.

```
curl -D - http://fli4l/admin/mein.cgi -u admin
```

<sup>12</sup>siehe <http://de.wikipedia.org/wiki/CURL>

## 8.7. Hochfahren, Herunterfahren, Einwählen und Auflegen unter fli4l

### 8.7.1. Bootkonzept

fli4l 2.0 sollte eine saubere Installation auf eine Festplatte oder ein CompactFlash(TM)-Medium bieten, aber auch eine Installation auf ein Zip-Medium oder die Erstellung einer bootfähigen CD-ROM sollte möglich sein. Zusätzlich sollte die Festplattenversion sich nicht grundlegend von einer Installation auf Diskette<sup>13</sup> unterscheiden.

Diese Anforderungen wurden realisiert, indem die Dateien des `opt.img`-Archivs aus der bisherigen RAM-Disk auf eine anderes Medium verlagert werden können. Dies kann eine Partition auf einer Festplatte bzw. einem CF-Medium sein. Dieses zweite Volume wird unter `/opt` eingehängt, und dort liegende Programme werden nur noch über symbolische Links in das RootFS integriert. Das entstehende Layout im RootFS-Dateisystem entspricht dann dem im `opt`-Verzeichnis der ausgepackten fli4l-Distribution mit einer Ausnahme – das `files`-Präfix entfällt. Die Datei `opt/etc/rc` ist dann also direkt unter `/etc/rc` zu finden, `opt/bin/busybox` unter `/bin/busybox`. Dass diese Dateien unter Umständen nur symbolische Verknüpfungen auf ein im Nur-Lese-Modus eingehängtes Volume sind, kann man ignorieren, solange man die Dateien nicht modifizieren möchte. Will man dies tun, muss man die Dateien vorher mit `mk_writable` (s. u.) schreibbar machen.

### 8.7.2. Start- und Stopp-Skripte

Skripte, die beim Hochfahren des Systems ausgeführt werden sollen, befinden sich in den Verzeichnissen `opt/etc/boot.d/` und `opt/etc/rc.d/` und werden auch in dieser Reihenfolge ausgeführt. Des Weiteren befinden sich in `opt/etc/rc0.d/` Skripte, die beim Herunterfahren des Systems ausgeführt werden.

**Wichtig:** *Da zum Ausführen dieser Skripte kein separater Prozess erzeugt wird, dürfen sie nicht mit „exit“ abgeschlossen werden. Ein solcher Befehl führt zum vorzeitigen Abbruch des Bootvorgangs!*

#### Start-Skripte in `opt/etc/boot.d/`

Skripte, die in diesem Verzeichnis liegen, werden als erstes ausgeführt. Ihre Aufgabe ist es, das Boot-Volume einzuhängen, die auf dem Boot-Medium liegende Konfigurationsdatei `rc.cfg` einzulesen und das Opt-Archiv zu entpacken. Je nach [Boot-Typ](#) (Seite 29) sind diese Skripte mehr oder weniger kompliziert und tun die folgenden Dinge:

- Laden von Hardware-Treibern (optional)
- Boot-Volume einhängen (optional)
- Konfigurationsdatei `rc.cfg` vom Boot-Volume einlesen und in die Datei `/etc/rc.cfg` schreiben
- Einhängen des Opt-Volumes (optional)

<sup>13</sup>Ursprünglich konnte fli4l auch von einer Diskette betrieben werden. Da fli4l inzwischen dafür zu groß geworden ist, wird dies nicht mehr unterstützt.

- Extrahieren des Opt-Archivs (optional)

Damit die Skripte überhaupt eine Chance haben, etwas über die fli4l-Konfiguration zu erfahren, wird die Konfigurationsdatei auch ins RootFS-Archiv unter `/etc/rc.cfg` eingebunden; die Konfigurationsvariablen in dieser Datei stehen den Start-Skripten in `opt/etc/boot.d/` direkt zur Verfügung. Nach dem Einhängen des Boot-Volumes wird die `/etc/rc.cfg` durch die Konfigurationsdatei vom Boot-Volume ersetzt, so dass den Start-Skripten in `opt/etc/rc.d/` (s. u.) die aktuelle Konfiguration vom Boot-Volume zur Verfügung steht. <sup>14</sup>

### Start-Skripte in `opt/etc/rc.d/`

Befehle, die immer beim Starten des Routers ausgeführt werden müssen, können in Skripten im Verzeichnis `opt/etc/rc.d/` abgelegt werden. Hierbei gelten folgende Konventionen:

1. Es gilt folgende Namenskonvention:

```
rc<dreistellige Zahl>.<Name des OPTs>
```

Die Skripte werden in aufsteigender Reihenfolge der Zahlen gestartet. Ist mehreren Skripten dieselbe Zahl zugeordnet, entscheidet die alphabetische Sortierung nach dem Punkt. Falls der Start eines Pakets erst nach einem anderen erfolgen darf, wird das durch die Zahl festgelegt.

Hier eine ungefähre Richtlinie, welche Nummern für welche Aufgaben verwendet werden sollten:

Nummer	Aufgabe
000-099	Grundsystem (Hardware, Zeitzone, Dateisystem)
100-199	Kernel-Module (Treiber)
200-299	externe Verbindungen (PPPoE, ISDN4Linux, PPTP)
300-399	Netzwerk (Routing, Interfaces, Paketfilter)
400-497	Server (DHCP, HTTPD, Proxy, etc.)
498-499	reserviert (Aktivierung des Circuit-Systems)
500-997	nach Belieben (ab hier können Skripte von Circuits kontrollierte Verbindungen nutzen und laufen möglicherweise parallel zu einer Einwahl)
998-999	reserviert (bitte nicht benutzen!)

2. In diesen Skripten *müssen* alle Funktionen, die das RootFS verändern, hinterlegt werden, etwa das Anlegen eines Verzeichnisses `/var/log/lpd`.
3. In diesen Skripten dürfen *keine* Schreibzugriffe auf Dateien erfolgen, die Teil des Opt-Archivs sein können, da diese Dateien auf einem im Nur-Lese-Modus eingehängten Volume liegen können. Muss man eine solche Datei modifizieren, muss man sie vorher mit Hilfe der Funktion `mk_writable` (s. u.) beschreibbar machen. Durch den Aufruf der Funktion

<sup>14</sup>Normalerweise sind diese beiden Dateien identisch. Eine Abweichung entsteht nur, wenn die Konfigurationsdatei auf dem Boot-Volume händisch editiert wird, etwa um die Konfiguration nachträglich abzuändern, ohne die fli4l-Archive neu zu bauen.

wird die Datei (wenn nötig) als beschreibbare Kopie im RootFS abgelegt. Ist die Datei bereits beschreibbar, bewirkt der `mk_writable`-Aufruf nichts.

**Wichtig:** `mk_writable` muss direkt auf Dateien im RootFS angewandt werden, nicht über den Umweg des `opt`-Verzeichnisses. Will man also `/usr/local/bin/foo` modifizieren, ruft man `mk_writable` mit dem Argument `/usr/local/bin/foo` auf.

4. Diese Skripte müssen vor der Ausführung der eigentlichen Befehle prüfen, ob das dazugehörige OPT auch aktiv ist. Das ist normalerweise durch eine einfache Fallunterscheidung erledigt:

```
if [ "$OPT_<OPT-Name>" = "yes" ]
then
    ...
    # Hier OPT starten!
    ...
fi
```

5. Um die Fehlersuche zu erleichtern, sollten die Skripte mit `begin_script` und `end_script` geklammert werden:

```
if [ "$OPT_<OPT-Name>" = "yes" ]
then
    begin_script F00 "configuring foo ..."
    ...
    end_script
fi
```

Die Fehlersuche einzelner Start-Skripte kann man dann einfach via `F00_DO_DEBUG='yes'` aktivieren.

6. Den Skripten stehen alle Konfigurationsvariablen direkt zur Verfügung. Im Abschnitt „Umgang mit Konfigurationsvariablen“ (Seite 376) wird erklärt, wie man von anderen Skripten aus auf die Konfigurationsvariablen zugreifen kann.
7. Der Pfad `/opt` darf auch nicht als Speicherplatz für Datenbestände der OPTs benutzt werden. Falls zusätzlicher Speicherplatz benötigt wird, sollte dem Benutzer über eine Konfigurationsvariable die Möglichkeit gegeben werden, einen geeigneten Pfad auszuwählen. Je nach Art der zu speichernden Daten (persistente oder transiente Daten) sind verschiedene Standard-Belegungen sinnvoll. So bieten sich für transiente Daten etwa Pfade unterhalb von `/var/run/` an; für persistente Daten sollte die Funktion `map2persistent` (Seite 376) in Kombination mit einer geeigneten Konfigurationsvariable verwendet werden.

### Stopp-Skripte in `opt/etc/rc0.d/`

Jeder Rechner muss mal heruntergefahren oder neu gestartet werden. Nun kann es vorkommen, dass man Vorgänge ausführen muss, bevor der Rechner heruntergefahren oder neu gestartet wird. Zum Herunterfahren und Neustarten sind die Befehle „halt“ bzw. „reboot“ zuständig.



Diese Befehle werden auch aufgerufen, wenn man im IMONC oder in der Web-GUI auf die entsprechenden Schaltflächen klickt.

Alle Stopp-Skripte liegen im Verzeichnis `opt/etc/rc0.d/`. Ihre Dateinamen werden analog zu den Start-Skripten gebildet. Sie werden ebenfalls in *aufsteigender* Reihenfolge der Zahlen ausgeführt.

### 8.7.3. Hilfsfunktionen

In `/etc/boot.d/base-helper` werden verschiedene Funktionen bereitgestellt, die von den Start- und anderen Skripten verwendet werden können. Das betrifft Dinge wie Unterstützung zur Fehlersuche, Laden von Kernel-Modulen oder Ausgabe von Meldungen. Die einzelnen Funktionen werden im Folgenden aufgelistet und kurz beschrieben.

#### Skript-Steuerung

**begin\_script <Symbol> <Meldung>:** Gibt eine Meldung aus und aktiviert die Fehlersuche im Skript mittels `set -x`, falls `<Symbol>_DO_DEBUG` auf „yes“ steht.

**end\_script:** Gibt eine Abschluss-Meldung aus und deaktiviert die Fehlersuche, falls sie mit `begin_script` aktiviert wurde. Für jeden `begin_script`-Aufruf muss es einen zugehörigen `end_script`-Aufruf geben (und umgekehrt).

#### Laden von Kernel-Modulen

**do\_modprobe [-q] <Modul> <Parameter>\*:** Lädt ein Kernel-Modul inkl. eventueller Parameter bei gleichzeitiger Auflösung der Modulabhängigkeiten. Der Parameter „-q“ verhindert, dass im Fehlerfall eine Meldung auf der Konsole ausgegeben und ins Boot-Protokoll geschrieben wird. Die Funktion liefert im Erfolgsfall den Rückgabewert null zurück und im Fehlerfall einen Wert ungleich null. Damit lässt sich Code schreiben, der ein Fehlschlagen des Ladens eines Kernel-Moduls geeignet behandelt:

```
if do_modprobe -q acpi-cpufreq
then
    # kein CPU-Frequenzsteuerung via ACPI
    log_error "CPU-Frequenzsteuerung via ACPI nicht verfügbar!"
    # [...]
else
    log_info "CPU-Frequenzsteuerung via ACPI aktiviert."
    # [...]
fi
```

**do\_modprobe\_if\_exists [-q] <Modulpfad> <Modul> <Parameter>\*:**  
Prüft, ob das Modul `/lib/modules/<Kernel-Version>/<Modulpfad>/<Modul>` existiert und ruft bei Vorhandensein die Funktion `do_modprobe` auf.

**Wichtig:** *Das Modul muss tatsächlich unter dem angegebenen Modulnamen existieren, der Modulname darf kein Alias sein. Bei einem Alias wird direkt `do_modprobe` aufgerufen.*

**Meldungen und Fehlerbehandlung**

**log\_info** <Meldung>: Schreibt eine Meldung auf die Konsole und nach /bootmsg.txt. Wird keine Meldung als Parameter übergeben, liest **log\_info** von der Standard-Eingabe. Die Funktion liefert als Rückgabewert immer null zurück.

**log\_warn** <Meldung>: Schreibt eine Warnmeldung auf die Konsole und nach /bootmsg.txt, wobei vor die Meldung die Zeichenkette **WARN:** gesetzt wird. Wird keine Meldung als Parameter übergeben, liest **log\_warn** von der Standard-Eingabe. Die Funktion liefert als Rückgabewert immer null zurück.

**log\_error** <Meldung>: Schreibt eine Fehlermeldung auf die Konsole und nach /bootmsg.txt, wobei vor die Meldung die Zeichenkette **ERR:** gesetzt wird. Wird keine Meldung als Parameter übergeben, liest **log\_error** von der Standard-Eingabe. Die Funktion liefert als Rückgabewert immer einen Wert ungleich null zurück.

**set\_error** <Meldung>: Gibt die Fehlermeldung aus und setzt eine interne Fehlervariable, das später via **is\_error** geprüft werden kann.

**is\_error**: Setzt die interne Fehlervariable zurück und liefert wahr zurück, falls sie vorher durch **set\_error** gesetzt wurde.

**Netzwerk-Funktionen**

**translate\_ip\_net** <Wert> <Variablenname> [<Ergebnisvariable>]: Ersetzt symbolische Referenzen in Parametern. Momentan finden folgende Übersetzungen statt:

**Host- oder Netzwerk-Adressen** werden nicht übersetzt

**any** wird durch 0.0.0.0/0 ersetzt

**dynamic** wird durch die dynamische IPv4-Adresse des Routers ersetzt; das ist die IPv4-Adresse, die der Router beim Einwählen über einen Circuit mit einer Default-Route zugewiesen bekommt

**IP\_NET\_x** wird durch das in der Konfiguration stehende Netzwerk ersetzt; referenziert die Variable einen Circuit, so wird das dem Circuit zugewiesene IPv4-Netz zurückgegeben

**IP\_NET\_x\_IPADDR** wird durch die in der Konfiguration stehende IP-Adresse ersetzt; referenziert die Variable einen Circuit, so wird die dem Circuit zugewiesene IPv4-Adresse zurückgegeben

**IP\_ROUTE\_x** wird durch das in der Konfiguration stehende geroutete Netzwerk ersetzt

**@<Hostname>** wird durch die in der Konfiguration für den angegebenen Host spezifizierte IP-Adresse ersetzt

**{<circuit>}** wird durch das dem Circuit zugewiesene IPv4-Netz ersetzt

Das Ergebnis der Übersetzung wird in der Variable gespeichert, deren Name im dritten Parameter übergeben wird; fehlt dieser Parameter, wird das Ergebnis in der Variable **res** gespeichert. Der Variablenname, der im zweiten Parameter übergeben wird, wird nur für Fehlermeldungen benutzt, falls die Übersetzung fehlschlägt; hier kann also vom Aufrufer die Quelle des zu übersetzenden Wertes angegeben werden. Im Fehlerfall wird dann eine Meldung wie

Unable to translate value '<Wert>' contained in <Variablenname>.

ausgegeben.

Der Rückgabewert ist null, falls die Übersetzung erfolgreich war, und ungleich null, falls ein Fehler aufgetreten ist.

## Diverses

**mk\_writable <Datei>:** Stellt sicher, dass die übergebene Datei beschreibbar ist. Befindet sich die Datei auf einem im Nur-Lese-Modus eingehängten Volume und ist lediglich über eine symbolische Verknüpfung ins Dateisystem eingebunden, wird eine lokale Kopie angelegt, die dann beschreibbar ist.

**list\_unique <Liste>:** Entfernt Duplikate aus der übergebenen Liste. Das Resultat wird in die Standard-Ausgabe geschrieben.

### 8.7.4. mdev-Regeln

Für OPTs ist es möglich, zusätzliche mdev-Regeln zu etablieren, die spezielle Aktionen beim Erscheinen oder Verschwinden bestimmter Geräte vornehmen. Das OPT\_AUTOMOUNT im hd-Paket verwendet beispielsweise eine solche Regel, um auftauchende Speichermedien automatisch einzuhängen. Will man eine zusätzliche mdev-Regel integrieren, muss man ein Skript der Form

```
/etc/mdev.d/mdev<Nummer>.<Name>
```

ins RootFS einbauen, wobei die Nummer ähnlich den Start- und Stopp-Skripten aus drei Ziffern bestehen muss und der Name beliebig gewählt werden kann. Innerhalb dieses Skriptes werden sämtliche Ausgaben an die Standardausgabe in die resultierende `/etc/mdev.conf` integriert. Ein Beispiel aus dem oben erwähnten OPT\_AUTOMOUNT:

```
#!/bin/sh
#-----
# /etc/mdev.d/mdev500.automount - mdev HD automounting rules      __FLI4LVER__
#
#
# Last Update:  $Id: dev_main_boot_dial.tex 51849 2018-03-06 14:55:21Z kristov $
#-----

cat <<"EOF"
#
# mdev500.automount
#

-SUBSYSTEM=block;DEVTYPE=partition;.+      0:0 660 */lib/mdev/automount

EOF
```

Zu der Syntax der Regeln sei auf den Dateikopf der `/etc/mdev.conf` sowie auf die mdev-Dokumentation unter <http://git.busybox.net/busybox/plain/docs/mdev.txt> verwiesen. Falls eine Regel ein Skript aufruft (wie `/lib/mdev/automount` im obigen Beispiel), dann hat es Zugriff auf alle Variablen des auslösenden Kernel-“uevent”s, insbesondere auf:

- ACTION (typischerweise **add** oder **remove**, seltener **change**)
- DEVPATH (sysfs-Pfad zu der betroffenen Komponente)
- SUBSYSTEM (das betroffene Kernel-Subsystem, siehe unten)
- DEVNAME (die betroffene Gerätedatei unter `/dev`; fehlt, wenn es nicht um zu erstellende oder löschende Geräte geht, sondern z.B. um Module)
- MDEV (wird von mdev auf den Namen der letztlich erzeugten Gerätedatei gesetzt)

Beispiele für Kernel-Subsysteme:

**block** Blockgeräte (Speichermedien) wie **sda** (erste Festplatte), **sr0** (erstes CD-Laufwerk) oder **ram1** (zweite RAM-Disk)

**input** Geräte für Eingaben von Tastatur, Maus etc. wie **input/event0**; welche Gerätedateien welchen Geräten zugeordnet sind, ist nicht festgelegt und muss im sysfs ermittelt werden

**mem** Geräte zum Zugriff auf den Speicher und Hardware-Ports wie **mem** und **ports**; hier fallen auch Pseudo-Geräte wie **zero** (liefert ununterbrochen das ASCII-Zeichen mit Wert null) und **null** (liefert nichts, verschluckt alles) darunter

**sound** diverse Geräte für die Tonausgabe, Benennung uneinheitlich

**tty** Geräte zum Zugriff auf physische und virtuelle Konsolen wie **tty1** (erste virtuelle Konsole) oder **ttyS0** (erste serielle Konsole)

Ein Beispiel für die ersten beiden seriellen Schnittstellen:

```
mdev[42]: 30.050644 add@/devices/pnp0/00:04/tty/ttyS0
mdev[42]: ACTION=add
mdev[42]: DEVPATH=/devices/pnp0/00:04/tty/ttyS0
mdev[42]: SUBSYSTEM=tty
mdev[42]: MAJOR=4
mdev[42]: MINOR=64
mdev[42]: DEVNAME=ttyS0
mdev[42]: SEQNUM=613

mdev[42]: 30.051477 add@/devices/platform/serial8250/tty/ttyS1
mdev[42]: ACTION=add
mdev[42]: DEVPATH=/devices/platform/serial8250/tty/ttyS1
mdev[42]: SUBSYSTEM=tty
mdev[42]: MAJOR=4
mdev[42]: MINOR=65
mdev[42]: DEVNAME=ttyS1
mdev[42]: SEQNUM=614
```

Ein Beispiel für eine angeschlossene MF II-Tastatur:

```
mdev[41]: 4.030653 add@/devices/platform/i8042/serio0/input/input0
mdev[41]: ACTION=add
mdev[41]: DEVPATH=/devices/platform/i8042/serio0/input/input0
mdev[41]: SUBSYSTEM=input
mdev[41]: PRODUCT=11/1/1/ab41
mdev[41]: NAME="AT Translated Set 2 keyboard"
mdev[41]: PHYS="isa0060/serio0/input0"
mdev[41]: PROP=0
```

## 8. Entwickler-Dokumentation

```
mdev[41]: EV=120013
mdev[41]: KEY=4 2000000 3803078 f800d001 feffffdf ffffffff ffffffff ffffffff
mdev[41]: MSC=10
mdev[41]: LED=7
mdev[41]: MODALIAS=input:b0011v0001p0001eAB41-e0,1,4,11,14,k71,72,73,74,75,76,77,79,
7A,7B,7C,7D,7E,7F,80,8C,8E,8F,9B,9C,9D,9E,9F,A3,A4,A5,A6,AC,AD,B7,B8,B9,D9,E2,ram4,10,
1,2,sfw
mdev[41]: SEQNUM=604
```

Ein Beispiel für ein geladenes USB-Kernelmodul (`uhci_hcd`):

```
mdev[41]: 6.537506 add@/module/uhci_hcd
mdev[41]: ACTION=add
mdev[41]: DEVPATH=/module/uhci_hcd
mdev[41]: SUBSYSTEM=module
mdev[41]: SEQNUM=633
```

Ein Beispiel für eine angeschlossene Festplatte:

```
mdev[41]: 7.267527 add@/devices/pci0000:00/0000:00:07.1/ata1/host0/target0:0:0:0/block/sda
mdev[41]: ACTION=add
mdev[41]: DEVPATH=/devices/pci0000:00/0000:00:07.1/ata1/host0/target0:0:0:0/block/sda
mdev[41]: SUBSYSTEM=block
mdev[41]: MAJOR=8
mdev[41]: MINOR=0
mdev[41]: DEVNAME=sda
mdev[41]: DEVTYPEDISK=disk
mdev[41]: SEQNUM=688
```

Dies ist eine ATA/IDE-Festplatte (`ata1`), die über den Gerätenamen `sda` angesprochen werden sollte.

Ein Beispiel für ein entferntes Blockgerät (die Zuordnung einer Image-Datei zu einer `fl4l-VM` wurde via `virsh detach-device` gelöst):

```
mdev[42]: 52.600646 remove@/devices/pci0000:00/0000:00:0a.0/virtio5/block/vdb/vdb1
mdev[42]: ACTION=remove
mdev[42]: DEVPATH=/devices/pci0000:00/0000:00:0a.0/virtio5/block/vdb/vdb1
mdev[42]: SUBSYSTEM=block
mdev[42]: MAJOR=254
mdev[42]: MINOR=17
mdev[42]: DEVNAME=vdb1
mdev[42]: DEVTYPEDISK=partition
mdev[42]: SEQNUM=776

mdev[42]: 52.644642 remove@/devices/virtual/bdi/254:16
mdev[42]: ACTION=remove
mdev[42]: DEVPATH=/devices/virtual/bdi/254:16
mdev[42]: SUBSYSTEM=bdi
mdev[42]: SEQNUM=777

mdev[42]: 52.644718 remove@/devices/pci0000:00/0000:00:0a.0/virtio5/block/vdb
mdev[42]: ACTION=remove
mdev[42]: DEVPATH=/devices/pci0000:00/0000:00:0a.0/virtio5/block/vdb
mdev[42]: SUBSYSTEM=block
mdev[42]: MAJOR=254
mdev[42]: MINOR=16
mdev[42]: DEVNAME=vdb
mdev[42]: DEVTYPEDISK=disk
mdev[42]: SEQNUM=778

mdev[42]: 52.644777 remove@/devices/pci0000:00/0000:00:0a.0/virtio5
mdev[42]: ACTION=remove
mdev[42]: DEVPATH=/devices/pci0000:00/0000:00:0a.0/virtio5
```

```

mdev[42]: SUBSYSTEM=virtio
mdev[42]: MODALIAS=virtio:d00000002v00001AF4
mdev[42]: SEQNUM=779

mdev[42]: 52.644973 remove@/devices/pci0000:00/0000:00:0a.0
mdev[42]: ACTION=remove
mdev[42]: DEVPATH=/devices/pci0000:00/0000:00:0a.0
mdev[42]: SUBSYSTEM=pci
mdev[42]: PCI_CLASS=10000
mdev[42]: PCI_ID=1AF4:1001
mdev[42]: PCI_SUBSYS_ID=1AF4:0002
mdev[42]: PCI_SLOT_NAME=0000:00:0a.0
mdev[42]: MODALIAS=pci:v00001AF4d00001001sv00001AF4sd00000002bc01sc00i00
mdev[42]: SEQNUM=780

```

Wie man sehen kann, sind bei einer solchen Entfernung diverse Kernel-Subsysteme involviert (hier `block`, `bdi`, `virtio` und `pci`).

### 8.7.5. ttyI-Geräte

Für die ttyI-Geräte (`/dev/ttyI0 ... /dev/ttyI15`), über welche die „Modem-Emulation“ der ISDN-Karte genutzt werden kann, existiert ein Zähler, um Konflikte zwischen verschiedenen Paketen, die diese Geräte nutzen, zu vermeiden. Hierzu wird beim Start des Routers die Datei `/var/run/next_ttyI` angelegt, die von den verschiedenen OPTs abgefragt und fortgezählt werden kann. Mit dem folgenden Beispielskript kann dieser Wert abgefragt, um eins erhöht und wieder für das nächste OPT exportiert werden.

```

ttydev_error=
ttydev=$(cat /var/run/next_ttyI)
if [ $ttydev -le 16 ]
then
    ttydev=$((ttydev + 1))          # ttyI device available? yes
    echo $ttydev >/var/run/next_ttyI # ttyI device + 1
else
    log_error "No ttyI device for <Name # save it
    log_error "deines OPTs> available!" # ttyI device available? no
    ttydev_error=true                # set error for later use
fi

if [ -z "$ttydev_error" ]
then
    ...                             # start OPT only if next tty device
    ...                             # was available to minimize error
    ...                             # messages and minimize the
    ...                             # risk of uncomplete boot
fi

```

### 8.7.6. Skripte beim Einwählen und Auflegen

#### Allgemeines

Nach dem Herstellen bzw. Trennen einer Circuit-Verbindung werden die Skripte in `/etc/ppp/` abgearbeitet. Hier können OPTs Aktionen hinterlegen, die nach dem Herstellen bzw. Auflegen der Verbindung nötig sind. Benannt werden die Dateien wie folgt:

```

ip-up<dreistellige Zahl>.<OPT-Name>
ip-down<dreistellige Zahl>.<OPT-Name>

```

Dabei werden die **ip-up**-Skripte nach dem *Aufbau* und die **ip-down**-Skripte nach dem *Abbau* der Verbindung ausgeführt.

**Wichtig:** In den **ip-down**-Skripten dürfen keine Aktionen ausgeführt werden, die zu einer erneuten Einwahl führen, da dadurch nur ein Dauer-Online-Zustand erreicht wird, was für Nicht-Flatrate-Benutzer ein teures Unterfangen ist.

**Wichtig:** Da für die einzelnen Skripte kein eigener Prozess erzeugt wird, dürfen auch diese Skripte nicht mit „exit“ abgeschlossen werden!

### Variablen

Durch das spezielle Aufrufkonzept stehen die folgenden Variablen den **ip-up**- und **ip-down**-Skripten zur Verfügung:

<code>real_interface</code>	die aktuelle Schnittstelle, also z. B. <code>ppp0</code> , <code>ippp0</code> , ...
<code>interface</code>	das IMOND-Interface, also <code>pppoe</code> , <code>ippp0</code> , ...
<code>tty</code>	verbundenes Terminal, möglicherweise leer!
<code>speed</code>	die Verbindungsgeschwindigkeit, bei ISDN z. B. 64000
<code>local</code>	die eigene IP-Adresse
<code>remote</code>	die IP-Adresse des Point-To-Point-Partners
<code>is_default_route</code>	gibt an, ob das aktuelle <b>ip-up</b> / <b>ip-down</b> für die Schnittstelle durchgeführt wird, über welche die Default-Route geht (kann „yes“ oder „no“ sein)

### Default-Route

Seit Version 2.1.0 werden die **ip-up**/**ip-down**-Skripte nicht nur für die Schnittstelle ausgeführt, über welche die Default-Route geht, sondern für alle Verbindungen, welche die **ip-up**- und **ip-down**-Skripte aufrufen. Um das alte Verhalten zu simulieren, muss in **ip-up**- und **ip-down**-Skripten die folgende Abfrage eingefügt werden:

```
# is a default-route-interface going up?
if [ "$is_default_route" = "yes" ]
then
    # die eigentlichen Aktionen
fi
```

Natürlich darf das neue Verhalten auch für spezielle Aktionen ausgenutzt werden.

## 8.8. Paket „template“

Um einiges von dem hier Beschriebenen etwas zu veranschaulichen, liegt der fli4l-Distribution das Paket „template“ bei. Dieses erklärt an kleinen Beispielen, wie:

- eine Konfigurationsdatei auszusehen hat (`config/template.txt`)
- eine Check-Datei geschrieben wird (`check/template.txt`)

- die erweiterten Prüfmöglichkeiten verwendet werden (`check/template.ext`)
- Konfigurationsvariablen für spätere Verwendung abgelegt werden können (`opt/etc/rc.d/rc999.template`)
- abgelegte Konfigurationsvariablen wieder ausgelesen werden (`opt/usr/bin/template_show_config`)

## 8.9. Aufbau des Boot-Datenträgers

Seit Version 1.5 wird das Programm `syslinux` zum Booten verwendet. Dieses hat den Vorteil, dass ein DOS-kompatibles Dateisystem auf dem Datenträger zur Verfügung steht.

Der Boot-Datenträger enthält folgende Dateien:

<code>ldlinux.sys</code>	der Urlader („Boot loader“) <code>syslinux</code>
<code>syslinux.cfg</code>	Konfigurationsdatei für <code>syslinux</code>
<code>kernel</code>	Linux-Kernel
<code>rootfs.img</code>	RootFS: enthält zum Booten nötige Programme
<code>opt.img</code>	Optionale Dateien: Treiber und Pakete
<code>rc.cfg</code>	Konfigurationsdatei mit den benutzten Variablen aus den Dateien des Konfigurationsverzeichnisses
<code>boot.msg</code>	Texte für das <code>syslinux</code> -Bootmenü
<code>boot_s.msg</code>	Texte für das <code>syslinux</code> -Bootmenü
<code>boot_z.msg</code>	Texte für das <code>syslinux</code> -Bootmenü
<code>hd.cfg</code>	Konfigurationsdatei zur Zuordnung der Partitionen

Durch das Skript `mkfli4l.sh` (bzw. `mkfli4l.bat`) werden zunächst die Dateien `opt.img`, `syslinux.cfg` und `rc.cfg` sowie das `rootfs.img` erzeugt. Die dafür nötigen Dateien ermittelt das Programm `mkfli4l` (im `unix-` bzw. `windows-`Unterverzeichnis). In den beiden Archiven sind die benötigten Kernel- und andere Pakete enthalten. Die Datei `rc.cfg` befindet sich sowohl im Opt-Archiv als auch auf dem Boot-Datenträger.<sup>15</sup>

Anschließend werden die Dateien `kernel`, `rootfs.img`, `opt.img` und `rc.cfg` zusammen mit den `syslinux`-Dateien auf den Datenträger kopiert.

Beim Booten von `fli4l` wird über das Skript `/etc/rc` die `rc.cfg` ausgewertet und das komprimierte `opt.img`-Archiv in die RootFS-RAM-Disk integriert (je nach Installationstyp werden dabei die Dateien direkt in die RootFS-RAM-Disk entpackt oder über symbolische Verknüpfungen eingebunden). Danach werden die Skripte in `/etc/rc.d/` in alphanumerischer Reihenfolge ausgeführt und somit die Treiber geladen und die Dienste gestartet.

## 8.10. Konfigurationsdateien

Hier werden die Dateien kurz aufgeführt, die vom `fli4l`-Router on-the-fly beim Booten erzeugt werden.

### 1. Konfiguration Provider

<sup>15</sup>Die Fassung im Opt-Archiv ist während der frühen Boot-Phase nötig, weil zu diesem Zeitpunkt das Boot-Volume noch nicht eingehängt ist.



- `etc/ppp/pap-secrets`
- `etc/ppp/chap-secrets`

## 2. Konfiguration DNS

- `etc/resolv.conf`
- `etc/dnsmasq.conf`
- `etc/dnsmasq_dhcp.conf`
- `etc/resolv.dnsmasq`

## 3. Hosts-Datei

- `etc/hosts`

## 4. imond-Konfiguration

- `etc/imond.conf`

### 8.10.1. Konfiguration Provider

Für den ausgesuchten Provider wird in `etc/ppp/pap-secrets` die User-ID und das Passwort angepasst.

Beispiel für Provider Planet-Interkom:

```
# Secrets for authentication using PAP
# client      server  secret          IP addresses
"anonymer"    *        "surfer"        *
```

Dabei ist im Beispiel „anonymer“ die USER-ID. Als Remote-Server wird prinzipiell jeder erlaubt (deshalb „\*“). „surfer“ ist das Passwort für den Provider Planet-Interkom.

### 8.10.2. Konfiguration DNS

Man kann den fli4l-Router als DNS-Server einsetzen. Warum dies sinnvoll und bei Windows-Rechnern im LAN sogar zwingend notwendig ist, wird in der Dokumentation des „base“-Pakets erläutert.

Die Resolver-Datei `etc/resolv.conf` enthält den Domainnamen und den zu verwendenden Nameserver. Sie hat folgenden Inhalt (wobei „domain.de“ nur ein Platzhalter für den Wert der Konfigurationsvariable `DOMAIN_NAME` ist):

```
search domain.de
nameserver 127.0.0.1
```

Der DNS-Server `dnsmasq` wird über die Datei `etc/dnsmasq.conf` konfiguriert. Sie wird beim Booten vom Skript `rc040.dns-local` sowie `rc370.dnsmasq` automatisch erzeugt und könnte wie folgt aussehen:

```
user=dns
group=dns
resolv-file=/etc/resolv.dnsmasq
no-poll
```

```
no-negcache
bogus-priv
log-queries
domain-suffix=lan.fli4l
local=/lan.fli4l/
domain-needed
expand-hosts
filterwin2k
conf-file=/etc/dnsmasq_dhcp.conf
```

### 8.10.3. Hosts-Datei

Diese Datei enthält eine Zuordnung von Host-Namen zu IP-Adressen. Diese Zuordnung ist jedoch nur lokal auf dem fli4l verwendbar, für andere Rechner im LAN ist sie nicht sichtbar. Diese Datei ist eigentlich überflüssig, wenn zusätzlich ein lokaler DNS-Server gestartet wird.

### 8.10.4. imond-Konfiguration

Die Datei `etc/imond.conf` wird unter anderem aus den Konfigurationsvariablen `CIRC_x_NAME`, `CIRC_x_ROUTE`, `CIRC_x_CHARGEINT` und `CIRC_x_TIMES` konstruiert. Sie kann aus bis zu 32 Zeilen (ohne die Kommentarzeilen) bestehen. Jede Zeile besteht aus acht Spalten:

1. Bereich Wochentag bis Wochentag
2. Bereich Stunde bis Stunde
3. Device (`ipppX` oder `isdnX`)
4. Circuit mit Default-Route: „yes“/„no“
5. Telefonnummer
6. Name des Circuits
7. Telefonkosten pro Minute in Euro
8. Zeittakt („Charge interval“) in Sekunden

Hier ein Beispiel:

#day	hour	device	defroute	phone	name	charge	ch-int
Mo-Fr	18-09	ippp0	yes	010280192306	Addcom	0.0248	60
Sa-Su	00-24	ippp0	yes	010280192306	Addcom	0.0248	60
Mo-Fr	09-18	ippp1	yes	019160	Compuserve	0.019	180
Mo-Fr	09-18	isdn2	no	0221xxxxxxx	Firma	0.08	90
Mo-Fr	18-09	isdn2	no	0221xxxxxxx	Firma	0.03	90
Sa-Su	00-24	isdn2	no	0221xxxxxxx	Firma	0.03	90

Weitere Erklärungen zum Least-Cost-Routing findet man in der Dokumentation des „base“-Pakets.

### 8.10.5. Die `/etc/.profile`-Datei

Die Datei `/etc/.profile` enthält benutzerdefinierte Einstellungen für die Shell. Um die Standard-Einstellungen zu überschreiben, ist es nötig, unterhalb seines Konfigurationsverzeichnis eine Datei `etc/.profile` zu erstellen. Dort können dann Einstellungen zum Prompt oder Abkürzungen (so genannte „Aliase“) eingetragen werden.

**Wichtig:** Diese Datei darf kein `exit` enthalten!

Beispiel:

```
alias ll='ls -al'
```

### 8.10.6. Skripte in `/etc/profile.d/`

In dem Verzeichnis `/etc/profile.d/` können Skripte abgelegt werden, die beim Starten einer Shell ausgeführt und damit die Umgebung für die Shell beeinflussen können. Typischerweise platzieren OPTs dort Skripte, welche spezielle Umgebungsvariablen setzen, die für die Programme des OPTs notwendig sind.

Falls sich sowohl Skripte in `/etc/profile.d/` befinden als auch die Datei `/etc/.profile` existiert, werden die Skripte in `/etc/profile.d/` nach dem Skript `/etc/.profile` ausgeführt.

## 8.11. Inkompatibilitäten zwischen 3.x und 4.x

Beim Umstellen von Paketen von Version 3.x auf 4.x sind die folgenden Dinge zu beachten:

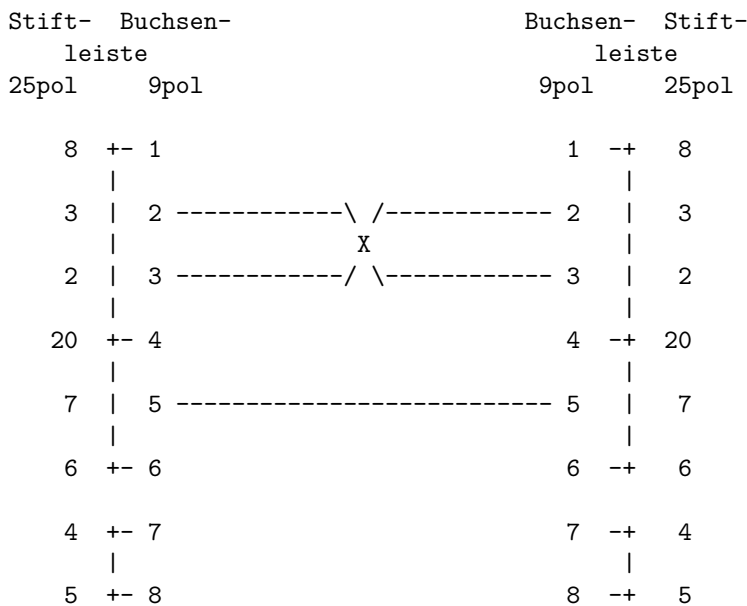
- Die zugrunde liegende `µClibc`-Bibliothek ist aktualisiert worden. Deswegen sollten alle Binärprogramme, die gegen eine ältere `µClibc` gebunden wurden, neu übersetzt werden. Das dafür nötige FBR (*fli4l Buildroot*) ist im `src`-Paket zu finden.
- Das Circuit-Konzept ist stark ausgebaut worden, so dass die Skripte in `/etc/ppp` häufiger aufgerufen werden als vorher (z.B. auch für alle konfigurierten Routen). Des Weiteren können jetzt dieselben Skripte für verschiedene Circuits parallel ausgeführt werden. Greift ein `ip-up`- oder ein `ip-down`-Skript auf eine globale Ressource zu (z.B. eine Datei, die von allen Circuits gleichermaßen genutzt wird), muss diese Ressource für die Dauer der Bearbeitung gesperrt und hinterher wieder freigegeben werden. Die dafür nötigen Funktionen `sync_lock_resource` und `sync_unlock_resource` werden in Abschnitt ?? beschrieben.
- Der Circuit und das Gerät `pppoe` existiert nur noch aus Kompatibilitätsgründen und sollte nicht mehr benutzt werden. Es repräsentiert den ersten konfigurierten PPPoE-Circuit bzw. die ihm zugrunde liegende Netzwerkschnittstelle. PPP-Circuits, die *keine* PPPoE-Circuits sind (dies trifft z.B. auf PPTP-, Fritz!DSL- oder UMTS-Circuits zu), werden über diesen Alias *nicht* mehr repräsentiert. Des Weiteren sollte in den Circuit-Skripten unterhalb von `/etc/ppp` die Variable `real_interface` nicht mehr genutzt werden. Statt dessen sollte die Variable `interface` verwendet werden. Eine Abbildung von der tatsächlichen PPP-Schnittstelle auf `pppoe` findet nicht mehr statt, da nicht mehr davon ausgegangen werden darf, dass es höchstens einen DSL-Circuit gibt. Es ist somit auch keine Prüfung mehr vorzunehmen, ob die Variable `interface` den Wert `pppoe` beinhaltet.

# A. Anhang zum Basispaket

## A.1. Nullmodemkabel

Für die Verwendung des optionalen Programmpakets [PPP](#) (Seite [225](#)) benötigt man ein Nullmodemkabel.

Dieses muss mindestens drei Adern haben. Hier die Anschluss-Belegung:



Bei den Steckern müssen die im Schaltbild gezeigte Brücken eingelötet werden.

## A.2. Serielle Konsole

fli4l kann ohne Monitor und Tastatur eingesetzt werden. Ein Nachteil davon ist, dass eventuelle Fehlermeldungen nicht bemerkt werden, weil sich nicht alle Meldungen über die syslog-Schnittstelle umleiten lassen.

Eine Möglichkeit ist die Umlenkung der Konsole-Meldungen auf seinen PC oder auf ein klassisches Terminal, nämlich über die serielle Schnittstelle. Die Konfiguration erfolgt über die Variablen [SER\\_CONSOLE](#) (Seite [35](#)), [SER\\_CONSOLE\\_IF](#) (Seite [36](#)) und [SER\\_CONSOLE\\_RATE](#) (Seite [36](#)).

Rechner mit älteren Mainboards/Karten unterstützen keine höheren Geschwindigkeiten als 38400 Baud. Deshalb sollte man es zunächst mit höchstens 38400 Baud probieren, bevor man sich an höhere Geschwindigkeiten heranwagt. Da lediglich Text-Ausgaben über die Konsole gehen, sind höhere Geschwindigkeiten eigentlich auch gar nicht notwendig.

Sämtliche Meldungen, die normalerweise auf der Konsole ausgegeben werden, werden nun auf die serielle Schnittstelle gelenkt – auch die Meldungen des Bootvorgangs!

Als Kabel zum Terminal oder PC mit Terminalemulation kommt ein [Nullmodemkabel](#) (Seite 404) zum Einsatz. Wir raten aber davon ab, ein Standard-Nullmodemkabel zu verwenden, weil dort normalerweise auch die Handshake-Leitungen verdrahtet sind. Ist das Terminal bzw. der PC abgeschaltet (oder die Terminalemulation nicht geladen), kann es bei Verwendung eines Standard-Nullmodemkabels zu einem Einfrieren von fli4l kommen!

Deshalb ist hier eine spezielle Verdrahtung notwendig, um fli4l auch mit abgeschaltetem Terminal betreiben zu können. Es wird dafür ein dreiadriges Kabel benötigt, wobei einige Kontakte an den Steckern überbrückt werden müssen. Siehe dazu bei [Nullmodemkabel](#) (Seite 404).

### A.3. Programme

Um Platz auf dem Bootmedium zu sparen, wird unter anderem das Paket “BusyBox” verwendet. Das Programm ist ein einzelnes Executable, welches die Standard-Unix-Programme

```
[, [[, arping, ash, base64, basename, bbconfig, blkid, bunzip2, bzip2,
cat, chgrp, chmod, chown, chroot, cmp, cp, cttyhack, cut, date, dd, df,
dirname, dmesg, dnsdomainname, echo, egrep, expr, false, fdflush, fdisk, find,
findfs, grep, gunzip, gzip, halt, hdparm, head, hostname, inetd, init, insmod,
ip, ipaddr, iplink, iproute, iprule, iptunnel, kill, killall, klogd, less, ln,
loadkmap, logger, ls, lsmmod, lzcat, makedevs, md5sum, mdev, mkdir, mknod,
mkswap, modprobe, mount, mv, nameif, nice, nslookup, ping, ping6, poweroff,
ps, pscan, pwd, reboot, reset, rm, rmmmod, sed, seq, sh, sleep, sort, swapoff,
swapon, sync, sysctl, syslogd, tail, tar, test, top, tr, true, tty, umount,
uname, unlzma, unxz, unzip, uptime, usleep, vi, watch, xargs, xzcat, zcat
```

nachbildet. Zumeist sind es jedoch “minimalistische” Implementationen, welche nicht den vollen Funktionsumfang abdecken, aber voll auf den bescheidenen Anforderungen von fli4l genügen.

BusyBox steht unter GPL und ist als Source komplett erhältlich unter

<http://www.busybox.net/>

### A.4. Andere i4l-Tools

Es gibt für isdn4linux viele weitere Tools, die auch fli4l bereichern würden. Das Problem ist leider der Platz! Bestimmt wäre isdnlog als Tool zum Berechnen der Online-Gebühren wesentlich geeigneter, jedoch ist isdnlog einfach zu fett!

imond braucht weniger als 10% des Platzes, übernimmt dabei Monitoring, Controlling und LC-Routing, wenn auch nicht alles ganz perfekt ist.

### A.5. Fehlersuche

Hilfreich bei der Fehlersuche sind natürlich einmal die Konsole-Outputs. Diese rauschen aber oft einfach so durch, dass man gar nicht mehr mitlesen kann. Hinweis: Mit SHIFT-BILD-RAUF kann man zurück-, mit SHIFT-BILD-RUNTER wieder vorblättern.

Falls im Betrieb des Routers Fehlermeldungen “try-to-free-pages” auftreten ist zuwenig für Programme nutzbares RAM übrig. Als Abhilfe stehen dann folgende Optionen zur Verfügung:

- mehr RAM einbauen
- weniger Opt-Pakete einsetzen
- eine Festplatteninstallation nach [Typ B](#) (Seite 17) durchführen

Auch proc-Dateien können bei der Fehlersuche helfen. z.B. gibt der Befehl

```
cat /proc/interrupts
```

die von den Treibern verwendeten Interrupts aus – nicht die tatsächlich von der Hardware belegten!

Weitere interessante Dateien unter /proc sind devices, dma, ioports, kmsg, meminfo, modules, uptime, version und pci (falls der Router einen PCI-Bus hat).

Meist liegt ein Verbindungsproblem bei ipppd vor, insbesondere bei der Authentifizierung. Dann helfen oft die Variablen

```
OPT_SYSLOGD='yes'
```

```
OPT_KLOGD='yes'
```

in config/base.txt und

```
ISDN_CIRC_x_DEBUG='yes'
```

in config/isdn.txt weiter.

## A.6. Literaturhinweise

- Computer Networks, Andy Tanenbaum
- TCP/IP Netzanbindung von PCs, Craig Hunt
- TCP/IP, Kevin Washburn, Jim Evans, Verlag: Addison-Wesley, ISBN: 3-8273-1145-4
- TCP/IP Netzanbindung von PCs, ISBN 3-930673-28-2
- TCP/IP Netzwerk Administration, ISBN 3-89721-110-6
- Linux-Anwenderhandbuch, ISBN 3-929764-06-7
- TCP/IP im Detail:  
<http://www.nickles.de/c/s/ip-adressen-112-1.htm>
- Generell das online Linuxanwenderhandbuch von Lunetix unter:  
<http://www.linux-ag.com/LHB/>
- Einführung in die Linux-Firewall: <http://www.little-idiot.de/firewall/>

## A.7. Präfixe

Bei den Einheiten richten die Präfixe in dieser Doku sich nach IEC 60027-2.

Siehe: <http://physics.nist.gov/cuu/Units/binary.html>.

## A.8. Gewähr und Haftung

Natürlich kann für das gesamte fli4l-Paket oder für Teile davon keine Gewähr dafür übernommen werden, dass es überhaupt funktioniert oder dass irgendeine Dokumentation in diesem Verzeichnis oder einem der Unterverzeichnisse korrekt ist.

Auch ist jede Haftung wegen evtl. entstandender Schäden oder Kosten ausgeschlossen!

## A.9. Danke

In diesem Abschnitt der Dokumentation soll all denen durch namentliche Nennung gedankt werden, die zur Entwicklung von fli4l beitragen bzw. beigetragen haben.

### A.9.1. Projektgründung

Meyer, Frank

Frank startete am 04.05.2000 das Projekt fli4l!

Siehe: <http://www.fli4l.de/home/eigenschaften/historie/>

### A.9.2. Entwickler- und Testteam

**Das fli4l-Team bilden (in alphabetischer Reihenfolge):**

Charrier, Bernard (*französische Übersetzung*)  
Eckhofer, Felix (*Dokumentation, Howtos*)  
Franke, Roland (*OW, FBR*)  
Hilbrecht, Claas (*VPN, Kernel*)  
Klein, Sebastian (*Kernel, Wlan*)  
Knipping, Michael (*Accounting*)  
Krister, Stefan (*Opt-Cop, lcd4linux*)  
Miksch, Gernot (*LCD*)  
Schiefer, Peter (*fli4l-CD, Opt-Cop, Webseite, Releasemanagement*)  
Schliesing, Manfred (*Tester*)  
Schulz, Christoph (*FBR, IPv6, Kernel*)  
Siebmanns, Harvey (*Dokumentation, englische Übersetzung*)  
Spieß, Carsten (*Dsltool, Hwsupp, Rrdtool, Webgui*)  
Vosselman, Arwin (*LZS-Kompression, Dokumentation*)  
Weiler, Manuela (*CD-Versand, Kassenwart*)  
Weiler, Marcel (*Qualitätsmanagement*)  
Wolters, Florian (*Firmware, Kernel*)

### A.9.3. Entwickler- und Testteam (nicht mehr aktive)

Arndt, Kai-Christian (*USB*)  
Bauer, Jürgen (*LCD-Package, fliwiz*)  
Behrends, Arno (*Support*)  
Blokland, Kees (*Englische Übersetzung*)  
Bork, Thomas (*lpdsrv*)  
Bußmann, Lars (*Tester*)  
Cerny, Carsten (*Webseite, fliwiz*)  
Dawid, Oliver (*dhcp, uClibc*)  
Ebner, Hannes (*QoS*)  
Fischer, Joerg (*Tester*)  
Frauenhoff, Peter (*Tester*)  
Grabner, Hans-Joerg (*imonc*)  
Grammel, Matthias (*Englische Übersetzung*)  
Gruetzmacher, Tobias (*Mini-httpd, imond, proxy*)  
Hahn, Joerg (*IPSEC*)  
Hanselmann, Michael (*Mac OS X/Darwin*)  
Hoh, Jörg (*Newsletter, NIC-DB, Veranstaltungen*)  
Hornung, Nicole (*Verein*)  
Horsmann, Karsten (*Mini-httpd, WLAN*)  
Janus, Frank (*LCD*)  
Kaiser, Gerrit (*Logo*)  
Karner, Christian (*PPTP-Package*)  
Klein, Marcus (*Problemfeedback*)  
Lammert, Gerrit (*HTML-Dokumentation*)  
Lanz, Ulf (*LCD*)  
Lichtenfeld, Nils (*QoS*)  
Neis, Georg (*fli4l-CD, Dokumentation*)  
Peiser, Steffen (*FAQ*)  
Peus, Christoph (*uClibc*)  
Pohlmann, Thorsten (*Mini-httpd*)  
Raschel, Tom (*IPX*)  
Reinard, Louis (*CompactFlash*)  
Resch, Robert (*PCMCIA, WLAN*)  
Schäfer, Harald (*HDD-Support*)  
Schmitts, Jupp (*Tester*)  
Strigler, Stefan (*GTK-Imonc, Opt-DB, NG*)  
Wallmeier, Nico (*Windows-Imonc*)  
Walter, Gerd (*UMTS*)  
Walter, Oliver (*QoS*)  
Wolter, Jean (*Paketfilter, uClibc*)  
Zierer, Florian (*Wunschliste*)



#### **A.9.4. Sponsoren**

Auch ist mittlerweile fli4l als Wort-/Bildmarke eingetragen. Folgende fli4l-Anwender (neben einigen, die nicht genannt werden wollten) haben geholfen das dafür nötige Geld zusammen zu bekommen:

Bebensee, Norbert  
Becker, Heiko  
Behrends, Arno  
Böhm, Stefan  
Brederlow, Ralf  
Groot, Vincent de  
Hahn, Olaf  
Hogrefe, Paul  
Holpert, Christian  
Hornung, Nicole  
Kuhn, Robert  
Lehnen, Jens  
Ludwig, Klaus-Ruediger  
Mac Nelly, Christa  
Mahnke, Hans-Jürgen  
Menck, Owen  
Mende, Stefan  
Mücke, Michael  
Roessler, Ingo  
Schiele, Michael  
Schneider, Juergen  
Schönleber, Suitbert  
Sennewald, Matthias  
Sternberg, Christoph  
Vollmar, Thomas  
Walter, Oliver  
Wiebel, Christian  
Woelk, Fabian

Seit einiger Zeit hat fli4l nun auch seine eigenen Sponsoren, die mit Ihrer (Hardware-)Spende die Weiterentwicklung von fli4l unterstützen. Dabei handelt es sich um Adapter, CompactFlash und Ethernetkarten.

Hardwarespender (in alphabetischer Reihenfolge):

Baglatzis, Stephanos  
Bauer, Jürgen  
Dross, Heiko  
Kappenhagen, Wenzel  
Kipka, Joachim  
Klopfer, Tom  
Peiser, Steffen  
Reichelt, Detlef  
Reinard, Louis  
Stärkel, Christopher

Weitere Sponsoren sind auf der fli4l-Homepage gelistet:

<http://www.fli4l.de/sonstiges/sponsoren/>

## A.10. Feedback

Kritik, Feedback und Zusammenarbeit ist jederzeit willkommen.

Die primäre Anlaufstelle dafür sind die fli4l-Newsgroups. Wer Probleme bei der Einrichtung eines fli4l-Routers hat, sollte sich erst FAQ, Howtos und NG-Archiv anschauen, bevor er sich an die Newsgroups wendet. Informationen über die verschiedenen Gruppen und die Netiquette findet man auf der fli4l-Webseite:

<http://www.fli4l.de/hilfe/newsgruppen/>

<http://www.fli4l.de/hilfe/faq/>

<http://www.fli4l.de/hilfe/howtos/>

Gerade weil für fli4l-Router meist ältere Hardware eingesetzt wird, kann es immer wieder mal zu Problemen kommen. Informationen können anderen fli4l-Usern bei Problemen mit der Hardware weiterhelfen, denn es gibt immer wieder Probleme mit den PC-Karten bzgl. I/O-Adressen, Interrupts und so weiter.

Auf der fli4l-Webseite wurde eine Netzwerkkarten-Datenbank eingerichtet, in die man z.B. die passenden Treiber für eine bestimmte Karte eintragen kann.

<http://www.fli4l.de/hilfe/nic-db/>

Viel Spaß mit fli4l!

## B. Anhänge der optionalen Pakete

### B.1. CHRONY - Benachrichtigung anderer Applikationen über Timewarps

Stellt chrony fest, dass die Uhr sehr weit von der tatsächlichen Uhrzeit abweicht, korrigiert chrony die Zeit in einem grossen Schritt und führt Scripts aus, um andere Anwendungen von diesem Zeitsprung zu informieren. Um z.B. den Imond von einem Zeitsprung zu informieren, macht chrony folgendes:

1. Scripte ins Archiv aufnehmen

Chrony fügt dem Archiv zwei Files hinzu:

```
imond yes etc/chrony.d/timewarp.sh mode=555 flags=sh
imond yes etc/chrony.d/timewarp100.imond mode=555 flags=sh
```

timewarp.sh führt alle Scripts im gleichen Verzeichnis aus, die dem Namen timewarp<3 ziffern>.<name> entsprechen.

2. Script zur Verfügung stellen

chrony nimmt folgendes Script mit ins Archiv auf:

```
# inform imond about time warp
imond-stat "adjust-time $timewarp 1"
```

Damit wird der imond über den Zeitsprung informiert und kann seine interne Zeitbasis anpassen.

### B.2. DYNDNS

#### B.2.1. Hinzufügen von neuen Providern

Das Hinzufügen von neuen Providern ist eigentlich sehr leicht, da die Update-Scripts komplett von den Provider-Daten getrennt sind. Für einen neuen Provider müssen folgende Dateien angepasst werden:

##### **Datei opt/etc/dyndns/provider.NAME**

Dies ist die Datei, in der definiert wird, wie ein Update bei diesem speziellen Provider funktioniert. Meistens besteht sie nur aus einer Liste von Variablen, da es aber ein ganz normales Shell-Script ist, können hier auch komplexere Operationen durchgeführt werden, das sollte aber selten nötig sein. In dieser Datei können folgende Variablen benutzt werden:

**\$ip** Die IP des Interfaces, das den dynamischen Hostnamen erhalten soll.

**\$host** Der komplette Hostname, wie ihn der Benutzer in seiner Konfiguration angegeben hat.

**\$subdom** Alle Komponenten des Hostnamen bis zum vorletzten Punkt (**name.provider.dom**)

**\$domain** Die letzten beiden Komponenten des Hostnamen (**name.provider.dom**)

**\$provider** Der symbolische Name des Providers, wie ihn der Benutzer in seiner Konfigurationsdatei angegeben hat.

**\$user** Der Benutzername für diesen Dienst.

**\$pass** Das dazugehörige Passwort.

Diese Variablen können zur klareren Abgrenzung gegenüber anderem Text mit geschweiften Klammern geschrieben werden, aus **\$ip** wird z.B. **\${ip}**. Bei Verwendung von Anführungszeichen ist zu beachten, dass innerhalb von einfachen Anführungszeichen die oben genannten Variablen *nicht* expandiert werden, bei doppelten Anführungszeichen schon. Als Faustregel kann man also sagen: Immer einfache Anführungszeichen benutzen, aber sobald man Variablen benutzt, doppelte Anführungszeichen benutzen.

Die folgenden Variablen müssen in dieser Datei definiert werden, damit das Paket weiß, wie ein Update bei dem entsprechenden Provider funktioniert:

**provider\_update\_type** Dies bestimmt die Art der Anfrage, die an den Server des Providers geschickt wird. Momentan werden unterstützt:

**http** Es wird automatisiert eine bestimmte Webseite des Providers abgerufen und so der DynDNS-Eintrag aktualisiert.

**netcat** Es wird einfach ein bestimmter Text an den Server des Providers geschickt, der das Update auslöst.

**gnudip** Ein relativ einfaches aber sicheres Updateverfahren, welches über zwei HTTP-Anfragen ausgeführt wird.

**provider\_host** Der Hostname des Providers, der bei einem Update kontaktiert wird.

**provider\_port** Der Port auf dem Host des Providers, der angesprochen werden soll. Der Standard-Port für HTTP ist 80.

Je nach Update-Typ müssen weitere Variablen angegeben werden:

**HTTP provider\_url** Hier wird die relative URL (ohne Hostname, aber mit / am Anfang zum Script des Providers abgelegt. Für Beispiele bitte die Dateien der anderen Provider ansehen.

**provider\_auth** (optional) Benötigt der Provider eine Anmeldung per Basic Authentication, so sind hier die entsprechenden Daten anzugeben. Das Format ist "USER:PASSWORD".

**Netcat provider\_data** Dies ist der Text, der an den Server des Providers geschickt wird. Siehe z.B. `provider.DYNEISFAIR`.

**GNUDip provider\_script** Der Pfad zum GNUDip-Script auf dem Server, dies ist meist etwas wie z.B. `'/cgi-bin/gdipupdt.cgi'`.

### Datei `opt/dyndns.txt`

Hier müssen eine oder mehr Zeilen für den neuen Provider eingefügt werden. Meistens reicht eine Zeile in der Art:

```
dyndns_%_provider    NAME    etc/dyndns/provider.NAME
```

Wird für den Provider HTTP und Basic Authentication benutzt, so braucht man noch das base64-Tool:

```
dyndns_%_provider    NAME    files/usr/local/bin/base64
```

Sollten noch andere Tools benötigt werden, bitte mir vorher eine Mail schicken, damit geprüft werden kann, ob das für das OPT\_DYNDNS geeignet ist.

### Datei `check/dyndns.exp`

In dieser Datei muss an der langen Zeile, die mit `DYNPROVIDER =` beginnt, der Providernamen mit einem senkrechten Strich von den anderen abgetrennt, hinten angefügt werden.

### Datei `doc/<Sprache>/tex/dyndns/dyndns_main.tex`

In der Dokumentation einen neuen Abschnitt eintragen. Auch hier sind die Provider alphabetisch nach dem Kurznamen, den der Benutzer in der Config-Datei eingibt, sortiert. Das prov-Makro ist am Anfang der Datei dokumentiert, genug Beispiele sollten vorhanden sein.

## B.2.2. Dank

Als allererstes möchten wir dem danken, der dieses Paket ins Leben gerufen hat und lange Zeit dieses Paket betreut hat: Thomas Müller (E-Mail: [opt\\_dyndns@s2h.cx](mailto:opt_dyndns@s2h.cx)) hat hier hervorragende Arbeit geleistet, ohne ihn wäre das Paket in der heutigen Form nicht möglich gewesen.

Desweiteren möchten wir auch Marcel Döring (E-Mail: [m@rcel.to](mailto:m@rcel.to)) danken, der das Paket einige Zeit lang gepflegt hat.

Bei der Entwicklung des Paketes haben sehr viele Leute geholfen und Ideen beigetragen. Mein Dank gilt allen diesen fleißigen Helfern.

Außerdem danken wir Frank Meyer und dem Rest des fli4l-Tems für ihre unermüdliche Arbeit, um den besten Router der Welt zu basteln (Bitte nicht ganz Ernst nehmen ;-).

Weiterhin möchten wir folgenden Leuten danken, die sich mit Tips, neuen Providern, Fehlerberichten, etc. an dem Paket beteiligt haben:

- Paul Bischof für den Provider AFRAID.
- Jens Fischer schrieb das Paket `opt_dtdns`, welches mich erst auf die Idee brachte, ein Paket für DynDNS.org zu schreiben.
- Till Jäger schrieb das Paket `opt_cjb`, welches in `opt_dyndns` übernommen habe.
- Tobias Gruetzmacher hat auf <http://portfolio16.de/index.de> Informationen zu weiteren DynDNS-Anbietern zusammengetragen, die hier verwendet werden.

- Die Anbieter dynamischer DNS, die auf ihren Webseiten zum Teil sehr gute, zum Teil weniger gute Beschreibungen des zu verwendenden Protokolls veröffentlicht haben.
- Die Programmierer diverser Update-Programme für DynDNS Anbieter, aus deren Code schamlos geklaut wurde. ;-)
- Heiko Ambos von dynaccess.de hat mich bei der Entwicklung der Unterstützung für diesen Anbieter unterstützt.
- Dennis Neuhäuser, der die Idee hatte, die Antworten der Dienste per Webserver verfügbar zu machen statt sie auf der Konsole auszugeben und auch gleich eine erste Implementation dafür geschickt hat.
- Lars Winkler der freundlicherweise die Änderungen, um das Paket unter 2.0pre2 zum Laufen zu bringen zur Verfügung gestellt hat.
- Markus Kraft und Tobias Gruetzmacher haben die Grundlage für die Anpassung an fli4l 2.0 gelegt.
- Georg Bärwald für die Daten zu Selfhost.de
- Mark C. Storck für die Daten zu Storck.org
- Arne Biermann für den Hinweis auf den Anbieter hn.org
- Detlef Paschke für die Daten zu dyn.ee und dyndns.dk
- Martin Kisser für seine Idee zum Vermeiden von Updates, wenn die IP sich nicht geändert hat.
- Björn Hoffmann für die Daten von DnsArt.com
- Christian Busch für die Daten von no-ip.com.
- Ralf Gill für das Update der Daten von selfhost.de.
- Michael (HeinB) für eine weitere Möglichkeit sich mit fli4l selbst in den Fuss zu schiessen. ;-)
- Marcus Mönnig, dito.

### **B.2.3. Lizenz**

Copyright ©2001-2002 Thomas Müller (E-Mail: [opt\\_dyndns@s2h.cx](mailto:opt_dyndns@s2h.cx))

Copyright ©2002-2003 Tobias Gruetzmacher (E-Mail: [fli4l@portfolio16.de](mailto:fli4l@portfolio16.de))

Copyright ©2004-201x fli4l-Team (E-Mail: [team@fli4l.de](mailto:team@fli4l.de))

Dieses Programm ist freie Software. Sie können es unter den Bedingungen der GNU General Public License, wie von der Free Software Foundation herausgegeben, weitergeben und/oder modifizieren, entweder unter Version 2 der Lizenz oder (wenn Sie es wünschen) jeder späteren Version.

Die Veröffentlichung dieses Programms erfolgt in der Hoffnung, dass es Ihnen von Nutzen sein wird, aber OHNE JEDE GEWÄHRLEISTUNG - sogar ohne die implizite Gewährleistung der

MARKTREIFE oder der EIGNUNG FÜR EINEN BESTIMMTEN ZWECK. Details finden Sie in der GNU General Public License.

Sie sollten eine Kopie der GNU General Public License zusammen mit diesem Programm erhalten haben. Falls nicht, schreiben Sie an die

Free Software Foundation Inc.  
59 Temple Place  
Suite 330  
Boston MA 02111-1307 USA.

Der Text der GNU General Public License ist auch im Internet unter <http://www.gnu.org/licenses/gpl.txt> veröffentlicht. Eine inoffizielle deutsche Übersetzung findet sich unter <http://www.gnu.de/documents/gpl.de.html> Diese Übersetzung soll jedoch nur zu einem besseren Verständnis der GPL verhelfen, rechtsverbindlich ist die englischsprachige Version.

### B.3. EASYCRON - Crontab in der Boot-Phase ergänzen

**Hinweis:** Die folgenden Ausführungen richten sich nur an Entwickler von Opt-Paketen für den *fl4l* Router.

Ab Version 2.1.7 stellt das rc-Script von Easycron die Funktion `add_crontab_entry()` zur Verfügung. Durch Aufruf dieser Funktion können andere rc-Scripts ab Startposition rc101 bis Startposition 949 Einträge an die Crontab anhängen. Am Ende der Boot-Phase mit dem Starten des cron Daemon sind die zusätzlichen Einträge aktiv.

```
add_crontab_entry time command [custom]
```

Mit `time` wird die Ausführungszeit in cron Notation übergeben, siehe die Manpage zu `crontab(5)` (<http://linux.die.net/man/5/crontab>). `command` enthält den auszuführenden Befehl. Der dritte Parameter `custom` ist optional. Mit ihm können Umgebungsvariablen passend zum Befehl gesetzt werden. Soll mehr als eine Variable gesetzt werden, sind die Zuweisungen durch `\\` zu trennen. Bitte **nicht** die Umgebungsvariable `PATH` verändern, da sonst nachfolgende `crontab` Einträge nicht mehr korrekt abgearbeitet werden können.

```
#
# example I: normal use, 2 parameters
#
    crontime="0 5 1 * *"
    croncmd="rotate_i_log.sh"

    add_crontab_entry "$crontime" "$croncmd"

#
# end of example I
#

#
# example II: extended use, 3 parameters and
#             multiple environment values
#
```

```
croncustom="source=/var/log/current \ dest=/mnt/data/log"
croncmd='cp $source $dest-`date +%Y%m%d`; > $source'
crontime="59 23 * * *"

add_crontab_entry "$crontime" "$croncmd" "$croncustom"

#
# end of example II
#
```

Die Richtigkeit der Einträge muß das aufrufende Script sicherstellen.

## **B.4. HD - Fehler im Zusammenhang mit Festplatten/CompactFlashes**

### **Problem:**

- der Router erkennt die Festplatte überhaupt nicht.

Mögliche Ursachen:

- über OPT\_HDDRV müssen eventuell zusätzliche Treiber für den HD-Controller definiert werden
- Platte ist falsch im BIOS eingetragen
- der Controller ist defekt oder abgeschaltet
- es wird bei der Installation die falsche Platte angegeben
- der Controller wird nicht von fli4l unterstützt. Manche Controller benötigen spezielle Treiber, die in fli4l nicht enthalten sind

### **Problem:**

- die Installation bricht ab
- nach einem Remote-Update des opt-Archives bootet der Router nicht mehr
- es gibt Fehlermeldungen beim Partitionieren oder Formatieren der Festplatte

Mögliche Ursachen:

- bei IDE-Festplatten könnte es an zu langen oder ungeeigneten IDE-Kabeln liegen
- bei älteren Festplatten ist die Einstellung der Transferrate/PIO-Mode im Bios oder auf dem Controller evtl. zu schnell für die Platte.
- ungeeigneter Chipsatz

Bemerkungen:



- bei Problemen mit den DMA-Einstellungen kann man versuchen im Paket base die Einstellung `LIBATA_NODMA='no'` zu setzen. (Der Standardwert ist hier 'yes'). Dies aktiviert DMA-Zugriffe an ATA Geräten.

**Problem:**

- nach der Installation bootet fli4l nicht von Festplatte

Mögliche Ursache:

- wenn der Bootvorgang von einem CF-Modul fehlschlägt sollte man prüfen ob das CF-Modul im Bios mit LBA oder LARGE erkannt wurde. Die richtige Einstellung für Module unter 512MB ist NORMAL oder CHS.
- es wird ein Adaptec 2940 Controller mit altem BIOS eingesetzt und das erweiterte Mapping für Festplatten über 1GB ist aktiv. Als Abhilfe kann man das BIOS des SCSI-Controllers aktualisieren oder das Mapping umschalten. **Beim Umschalten des Mappings gehen alle Daten auf der Platte verloren!**

**Problem:**

- Windows sagt während des Erstellens einer CF-Card: „Medium im Laufwerk (X:) besitzt kein FAT. [Abbruch]“.

Mögliche Ursache:

- Die Compactflash wurde zu früh / ohne Abmeldung aus dem Reader entfernt. Windows hatte den letzten Schreibvorgang noch nicht abgeschlossen, das Dateisystem ist nun beschädigt. Erstelle die CompactFlash nochmals direkt am fli4l mittels HD-Install.

## **B.5. HTTPD**

### **B.5.1. Zusätzliche Einstellungen**

Diese Einstellungen stehen normalerweise nicht in der Konfigurationsdatei, müssen also hinzugefügt werden, wenn sie benötigt werden.

**HTTPD\_USER** Mit dieser Option ist es möglich, den Webserver mit den Rechten eines anderen Benutzers als „root“ laufen zu lassen. Dies ist besonders sinnvoll, wenn der Webserver benutzt wird, um andere Seiten als das Admin-Interface bereitzustellen. Achtung: Es kann sein, dass einige Scripts, die Zugriff auf Konfigurationsdateien brauchen, dann nicht mehr laufen. Die Standard-Scripts dieses Pakets laufen unter jedem Benutzer.

### **B.5.2. Allgemeine Bemerkungen**

Wenn man TELMOND installiert hat, werden auf der Status- und der Calls- Seite die Telefonnummern der Anrufer angezeigt. Eine Namenszuordnung lässt sich in der Datei `opt/etc/phonebook` vornehmen. Diese Datei hat das gleiche Format wie die Telefonnummern-datei vom IMONC. Es können also Telefonbücher zwischen IMONC und Router ausgetauscht werden. Das Format jeder Zeile ist dabei „Telefonnummer=Name[,WAV-Datei]“ (ohne die

Anführungszeichen). Die WAV-Datei wird aber nur vom IMONC benutzt und vom Webserver ignoriert.

Das komplette Webinterface ist seit der Version 2.1.12 auf ein Framefreies Design mit CSS umgestellt worden. Alte Browser könnten damit Probleme haben. Allerdings hat das den Vorteil, dass man das Aussehen der Oberfläche fast beliebig verändern kann, einfach indem man die CSS-Dateien (im wesentlichen /opt/srv/www/css/main.css) anpasst.

Das Webserver-Paket wurde von Thorsten Pohlmann (E-Mail: [pohlmann@tetronik.com](mailto:pohlmann@tetronik.com)) erstellt und wird zur Zeit von Tobias Gruetzmacher (E-Mail: [fli4l@portfolio16.de](mailto:fli4l@portfolio16.de)) gepflegt. Das neue Design (seit der Version 2.1.12) wurde von Helmut Hummel (E-Mail: [hh@fli4l.de](mailto:hh@fli4l.de)) realisiert.

## B.6. HWSUPP - Geräteabhängige Einstellungen

### B.6.1. Verfügbare LED-Devices

Je nach HWSUPP\_TYPE sind verschiedene LED-Devices verfügbar. Bei nicht aufgeführter Hardware sind die PC-Tastatur LEDs wie bei [generic-pc](#) verfügbar.

Zusätzlich LED-Devices können z.B. auf WLAN-Karten verfügbar sein. Die gültigen Namen der LED-Devices ermittelt man mittels Eingabe von `ls /sys/class/leds/` z.B. per ssh auf der Router-Console.

#### **sim**

LED Simulation, erzeugt Eintrag im syslog:

- `simu::1`
- ...
- `simu::8`

#### **generic-pc**

PC-Tastatur LEDs:

- `inputX::capslock`
- `inputX::numlock`
- `inputX::scrolllock`

#### **generic-acpi**

PC-Tastatur-LEDs, wie [generic-pc](#)

#### **generic-acpi-coretemp**

PC-Tastatur-LEDs, wie [generic-pc](#)

#### **pcengines-alix**

- alix::1
- alix::2
- alix::3

#### **pcengines-apu**

- apu::1
- apu::2
- apu::3

#### **pcengines-apu2**

- apu::1
- apu::2
- apu::3

#### **pcengines-wrap**

- wrap::1
- wrap::2
- wrap::3

#### **rpi**

- led0

#### **soekris-net4801**

- net48xx::error

#### **soekris-net5501**

- net5501::error

### **B.6.2. Verfügbare Button-Devices**

Je nach HWSUPP\_TYPE sind verschiedene GPIO-Devices für Taster vorbelegt.

#### **generic-pc und generic-acpi**

- evdev:isa0060/serio0/input0, beliebige (verfügbare) Taste

Zu beachten ist, dass Tasten*kombinationen* nicht möglich sind. Man kann also den Router nicht via ALT+F4 o.ä. herunterfahren.

#### **pcengines-alix**

- evdev:gpio-keys-polled/input0, Taste 408 (Restart)

#### **pcengines-apu**

- evdev:gpio-keys-polled/input0, Taste 408 (Restart)

#### **pcengines-apu2**

- evdev:gpio-keys-polled/input0, Taste 408 (Restart)

#### **pcengines-wrap**

- evdev:gpio-keys-polled/input0, Taste 408 (Restart)

#### **soekris-net5501**

- evdev:gpio-keys-polled/input0, Taste 408 (Restart)  
Der Taster ist am Soekris-Gehäuse mit “Reset” beschriftet.  
Achtung: Der Taster muss im BIOS freigeschaltet werden.

### **B.6.3. Hinweise zu spezieller Hardware**

#### **pcengines-alix**

Beim Alix führt ein fehlerhafter Treiber für den lm90 Temperatursensor nach einiger Zeit zum Ausfall der Temperaturanzeige.

Als Workaround wird der lm90 Treiber entladen und wieder neu geladen. Dies geschieht automatisch per cron-Job. Dazu muss das Paket easycron geladen werden (OPT\_EASYCRON='yes').

## **B.7. HWSUPP - Konfigurations-Beispiele**

### **B.7.1. generic-pc**

```
OPT_HWSUPP='yes'
HWSUPP_TYPE='generic-pc'

HWSUPP_WATCHDOG='no'
HWSUPP_CPUFREQ='no'

HWSUPP_LED_N='3'
HWSUPP_LED_1='ready'
HWSUPP_LED_1_DEVICE='input1::numlock'
HWSUPP_LED_2='online'
HWSUPP_LED_2_DEVICE='input1::capslock'
HWSUPP_LED_3='wlan'
HWSUPP_LED_3_DEVICE='input1::scrolllock'
HWSUPP_LED_3_WLAN='wlan0'
```

```
HWSUPP_BUTTON_N='0'
```

### B.7.2. pcengines-apu

```
OPT_HWSUPP='yes'
```

```
HWSUPP_TYPE='pcengines-apu'
```

```
HWSUPP_WATCHDOG='yes'
```

```
HWSUPP_CPUFREQ='yes'
```

```
HWSUPP_CPUFREQ_GOVERNOR='ondemand'
```

```
HWSUPP_LED_N='3'
```

```
HWSUPP_LED_1='ready'
```

```
HWSUPP_LED_1_DEVICE='apu::1'
```

```
HWSUPP_LED_2='wlan'
```

```
HWSUPP_LED_2_DEVICE='apu::2'
```

```
HWSUPP_LED_2_WLAN='wlan0'
```

```
HWSUPP_LED_3='online'
```

```
HWSUPP_LED_3_DEVICE='apu::3'
```

```
HWSUPP_BUTTON_N='1'
```

```
HWSUPP_BUTTON_1='wlan'
```

```
HWSUPP_BUTTON_1_DEVICE='evdev:gpio-keys-polled/input0'
```

```
HWSUPP_BUTTON_1_DEVICE_KEY='408'
```

```
HWSUPP_BUTTON_1_PARAM='wlan0'
```

### B.7.3. pcengines-apu mit GPIOs

```
OPT_HWSUPP='yes'
```

```
HWSUPP_TYPE='pcengines-apu'
```

```
HWSUPP_WATCHDOG='yes'
```

```
HWSUPP_CPUFREQ='yes'
```

```
HWSUPP_CPUFREQ_GOVERNOR='ondemand'
```

```
HWSUPP_LED_N='5'
```

```
HWSUPP_LED_1='ready'
```

```
HWSUPP_LED_1_DEVICE='apu::1'
```

```
HWSUPP_LED_2='wlan'
```

```
HWSUPP_LED_2_DEVICE='apu::2'
```

```
HWSUPP_LED_2_WLAN='wlan0'
```

```
HWSUPP_LED_3='online'
```

```
HWSUPP_LED_3_DEVICE='apu::3'
```

```
HWSUPP_LED_4='trigger'
```

```
HWSUPP_LED_4_PARAM='phy0rx'
```

```
HWSUPP_LED_4_DEVICE='gpio::237'
HWSUPP_LED_5='trigger'
HWSUPP_LED_5_PARAM='phy0tx'
HWSUPP_LED_5_DEVICE='gpio::245'

HWSUPP_BUTTON_N='2'
HWSUPP_BUTTON_1='wlan'
HWSUPP_BUTTON_1_DEVICE='evdev:gpio-keys-polled/input0'
HWSUPP_BUTTON_1_DEVICE_KEY='408'
HWSUPP_BUTTON_1_PARAM='wlan0'
HWSUPP_BUTTON_2='online'
HWSUPP_BUTTON_2_DEVICE='gpio::236' # für Linux-Kernel < 3.18
HWSUPP_BUTTON_2_DEVICE='gpio::492' # für Linux-Kernel >= 3.18 (x+256)
```

## B.8. HWSUPP - Blinkfolge

Die folgenden Blinkfolgen werden während des Bootvorgangs angezeigt:

```

1.  ⊗                               ⊗                               ...
2.  ⊗      ⊗                       ⊗      ⊗                       ...
3.  ⊗      ⊗      ⊗               ⊗      ⊗      ⊗               ...
4.  ⊗      ⊗      ⊗      ⊗       ⊗      ⊗      ⊗      ⊗       ...
```

Während der Abarbeitung von rc002.\* bis rc250.\* wird die erste Folge angezeigt (1 \* Blinken - Pause),  
 von rc250.\* bis rc500.\* die zweite (2 \* Blinken - Pause),  
 von rc500.\* bis rc750.\* die 3. und  
 von rc750.\* bis zum Ende des Bootvorgangs die 4. Folge (Dauerblinken).

## B.9. HWSUPP - Tasten-Codes

Die folgende Tabelle stellt die verschiedenen Tasten-Codes zusammen mit der jeweiligen Taste bei der deutschen, englischen und französischen Tastenbelegung dar. Die Abkürzung “NB” steht für “Nummernblock” und bezeichnet eine Taste im rechten abgesetzten Bereich der Tastatur. Ein Eintrag “—” bezeichnet eine Taste, die in der jeweiligen Belegung nicht existiert. Tasten-Codes, die bei allen drei dargestellten Tastaturbelegungen gar nicht vorkommen (dies gilt z.B. für diverse Tasten japanischer oder chinesischer Tastaturen), wurden gleich komplett weggelassen.

Zuerst folgt eine Tabelle mit den Standard-Tasten der IBM AT-Tastaturen mit 101 bzw. 102 Tasten.

Code	dt.	engl.	frz.
1	Esc	Esc	Esc
2	1	1	&
3	2	2	é
4	3	3	"

## B. Anhänge der optionalen Pakete

Code	dt.	engl.	frz.
5	4	4	,
6	5	5	(
7	6	6	-
8	7	7	è
9	8	8	-
10	9	9	ç
11	0	0	à
12	ß	-	)
13	?	=	=
14	Rückschritt ←		
15	Tabulator		
16	Q	Q	A
17	W	W	Z
18	E	E	E
19	R	R	R
20	T	T	T
21	Z	Y	Y
22	U	U	U
23	I	I	I
24	O	O	O
25	P	P	P
26	Ü	[	^
27	+	]	\$
28	Enter		
29	linke Strg-Taste		
30	A	A	Q
31	S	S	S
32	D	D	D
33	F	F	F
34	G	G	G
35	H	H	H
36	J	J	J
37	K	K	K
38	L	L	L
39	Ö	;	M
40	Ä	,	ù
41	^	‘	2
42	linke Umschalttaste		
43	#	\	*
44	Z	Z	W
45	X	X	X
46	C	C	C
47	V	V	V
48	B	B	B

## B. Anhänge der optionalen Pakete

Code	dt.	engl.	frz.
49	N	N	N
50	M	M	,
51	,	,	;
52	.	.	:
53	–	/	!
54	rechte Umschalttaste		
55	* (NB)	* (NB)	* (NB)
56	linke Alt-Taste		
57	Leertaste		
58	Feststelltaste		
59	F1	F1	F1
60	F2	F2	F2
61	F3	F3	F3
62	F4	F4	F4
63	F5	F5	F5
64	F6	F6	F6
65	F7	F7	F7
66	F8	F8	F8
67	F9	F9	F9
68	F10	F10	F10
69	Num ↓	Num Lock	Verr num
70	Rollen ↓	Scroll Lock	Arrêt Défil
71	7 (NB)	7 (NB)	7 (NB)
72	8 (NB)	8 (NB)	8 (NB)
73	9 (NB)	9 (NB)	9 (NB)
74	– (NB)	– (NB)	– (NB)
75	4 (NB)	4 (NB)	4 (NB)
76	5 (NB)	5 (NB)	5 (NB)
77	6 (NB)	6 (NB)	6 (NB)
78	+ (NB)	+ (NB)	+ (NB)
79	1 (NB)	1 (NB)	1 (NB)
80	2 (NB)	2 (NB)	2 (NB)
81	3 (NB)	3 (NB)	3 (NB)
82	0 (NB)	0 (NB)	0 (NB)
83	, (NB)	. (NB)	. (NB)
86	<	—	<
87	F11	F11	F11
88	F12	F12	F12
96	Enter (NB)		
97	rechte Strg-Taste		
98	÷ (NB)	/ (NB)	/ (NB)
99	Druck	Print Screen	Impr écran
100	rechte Alt-Taste (AltGr)		
102	Pos 1	Home	↖



Code	dt.	engl.	frz.
103	↑	↑	↑
104	Bild ↑	Page Up	↑
105	←	←	←
106	→	→	→
107	Ende	End	Fin
108	↓	↓	↓
109	Bild ↓	Page Down	↓
110	Einfüg	Insert	Inser
111	Entf	Delete	Suppr
119	Pause	Pause	Pause

Es schließt sich eine Tabelle mit zusätzlichen Tasten an. Nicht alle Tastaturen bieten diese Tasten an. Einige werden typischerweise nur von speziellen Hardware-Treibern generiert, etwa die **Restart**-Taste, die einen Druck auf den Reset-Schalter darstellt.

Code	dt.	engl.	frz.
116	Power	Power	Power
183	F13	F13	F13
184	F14	F14	F14
185	F15	F15	F15
186	F16	F16	F16
187	F17	F17	F17
188	F18	F18	F18
189	F19	F19	F19
190	F20	F20	F20
191	F21	F21	F21
192	F22	F22	F22
193	F23	F23	F23
194	F24	F24	F24
408	Restart	Restart	Restart

## B.10. HWSUPP - Hinweise für Paket-Entwickler

Im folgenden ist beschrieben was ein Paket-Entwickler zu tun hat, um Button- oder LED-Funktionalität zu einem Paket hinzuzufügen<sup>1</sup>.

### B.10.1. LED-Erweiterungen

#### LED-Typ

In der Datei `check/myopt.exp` wird die Liste der erlaubten LED-Typen die in `HWSUPP_LED_x` eingetragen werden können erweitert.

Beispiel:

```
+HWSUPP_LED_TYPE(OPT_MYOPT) = 'myopt'
```

<sup>1</sup>Wenn man im WLAN-Paket nach `##HWSUPP##` sucht so findet man die anzupassenden Stellen.

```
: ', myopt'
```

### Parameterprüfung

In der Datei `check/myopt.ext` werden die Parameter die für den neuen LED-Typen in `HWSUPP_LED_x_PARAM` eingetragen werden können geprüft.

Beispiel:

```
if (opt_hwsupp)
then
    depends on hwsupp version 4.0

    foreach i in hwsupp_led_n
    do
        set action=hwsupp_led_%[i]
        set param=hwsupp_led_%_param[i]
        if (action == "myopt")
        then
            if (!(param =~ "(RE:MYOPT_LED_PARAM)"))
            then
                error "When HWSUPP_LED_\${i}='myopt', ...
                        must be entered in HWSUPP_LED_\${i}_PARAM"
            fi
        fi
    done
fi
```

### LED schalten

Um eine LED zu schalten ist in einem eigenen Skript (z.B. `/usr/bin/<opt>_setled`) das Kommando `/usr/bin/hwsupp_setled <LED> <Status>/` aufzurufen.

Die LED-Nummer kann aus `/var/run/hwsupp.conf` ausgelesen werden.

Als Status ist `off`, `on` oder `blink` zu übergeben.

Beispiel:

```
if [ -f /var/run/hwsupp.conf ]
then
    . /var/run/hwsupp.conf
    [ 0$hwsupp_led_n -eq 0 ] || for i in `seq 1 $hwsupp_led_n`
    do
        eval action=\$hwsupp_led_\${i}
        eval param=\$hwsupp_led_\${i}_param
        if [ "$action" = "<opt>" ]
        then
            if [ <myexpression> ]
            then
                /usr/bin/hwsupp_setled $i on
            else
```

```
        /usr/bin/hwsupp_setled $i off
    fi
fi
done
fi
```

Den aktuellen Zustand einer LED kann man mit `/usr/bin/hwsupp_getled <LED>/` abfragen. Es wird je nach Status `off`, `on` oder `blink` ausgegeben.

### B.10.2. Button-Erweiterungen

### B.10.3. Button-Aktion

In der Datei `check/myopt.exp` wird die Liste der erlaubten Button-Typen die in `HWSUPP_BUTTON_x` eingetragen werden können erweitert.

Beispiel:

```
+HWSUPP_BUTTON_TYPE(OPT_MYOPT) = 'myopt'
                                : ', myopt'
```

### Parameterprüfung

In der Datei `check/myopt.ext` werden die Parameter, die für den neuen Button-Typen in `HWSUPP_BUTTON_x_PARAM` eingetragen werden können, geprüft.

Beispiel:

```
if (opt_hwsupp)
then
    depends on hwsupp version 4.0

    foreach i in hwsupp_button_n
    do
        set action=hwsupp_buttonn_%[i]
        set param=hwsupp_button_%_param[i]
        if (action == "myopt")
        then
            add_to_opt "files/usr/bin/myopt_keyprog" "mode=555 flags=sh"
            if (!(param =~ "(RE:MYOPT_BUTTON_PARAM)"))
            then
                error "When HWSUPP_BUTTON_\${i}='myopt', ...
                        must be entered in HWSUPP_BUTTON_\${i}_PARAM"
            fi
        fi
    done
fi
```

### Button-Funktion

Wenn eine Taste gedrückt wird, wird die Datei `/usr/bin/myopt_keyprog` ausgeführt.

Als Parameter wird er Inhalt von `HWSUPP_BUTTON_x_PARAM` übergeben  
Beispiel:

```
##TODO## example
```

## B.11. ISDN

### B.11.1. Technische Details zu Einwahl und Routing bei ISDN

Dieses Kapitel ist nur für Leute interessant, die ein wenig verstehen wollen, was intern passiert, die spezielle Konfigurationswünsche haben oder die nach der Lösung für Probleme suchen. Andere sollten dieses Kapitel bitte *nicht* lesen.

Nach dem Herstellen einer Verbindung zum Provider konfiguriert der `ipppd`-Daemon, der diese Verbindung hergestellt hat, das Interface neu, um die ausgehandelten IP-Adressen zu setzen. Dabei werden vom Linux-Kern automatisch auch Routen gesetzt, die der Remote-IP und der Netzmaske entsprechen und vorhandene, spezielle Routen werden gelöscht. Wird keine Netzmaske vorgegeben, leitet der `ipppd` aus der Remote-IP die Netzmaske ab (er benutzt dazu die Überholte Einteilung in Class A,B und C Subnetze). Das Verschwinden der Routen und die automatisch gesetzten neuen Routen haben immer wieder für Probleme gesorgt:

- Firmennetze waren nicht mehr erreichbar, weil die Routen verschwunden waren oder von den gesetzten neuen Routen überlagert wurden
- Interfaces wählten sich scheinbar ohne Grund ein, da ein Paket statt über die default Route über die vom Kern generierte Route auf ein anderes Interface ging
- ...

Daher wird nunmehr versucht, diese unerwünschten Routen zu verhindern.  
Dazu werden folgende Dinge geändert:

- `remote ip` wird auf `0.0.0.0` gesetzt, wenn nichts anderes spezifiziert ist. Dadurch verschwinden die Routen, die beim Konfigurieren des Interfaces vom Kern eingerichtet werden.
- zusätzlich angegebene Routen über den Circuit werden in einer Datei zwischengespeichert
- wird eine Netzwerkmaske für den Circuit angegeben, wird diese an den `ipppd` weitergereicht, damit der sie nach Aushandeln der IP für die Konfiguration des Interfaces (und damit für die Generierung von Routen) nutzt.
- nach dem Einwählen werden die zwischengespeicherten Routen des Circuits ausgelesen und wieder gesetzt (sie wurden vom Kern beim Neukonfigurieren des Interfaces durch `ipppd` gelöscht)
- nach dem Auflegen wird das Interface wieder neu konfiguriert und die Routen werden neu gesetzt um die Ausgangssituation wieder herzustellen.

Die Konfiguration der Circuits sieht dann wie folgt aus:

- item default route

```
ISDN_CIRC_%_ROUTE='0.0.0.0'
```

Ist der Circuit ein lcr circuit und gerade “aktiv”, wird eine default route auf diesen Circuit (bzw. das dazugehörige Interface) gesetzt. Nach dem Einwählen erscheint eine Host-Route zum Provider, die nach dem Auflegen wieder verschwindet.

- spezielle Routen

```
ISDN_CIRC_%_ROUTE='network/netmaskbits'
```

Es werden die angegebenen Routen auf den Circuit (bzw. das dazugehörige Interface) eingerichtet. Nach dem Einwählen werden die von Kern gelöschten Routen wieder hergestellt und es gibt eine Host-Route zum Einwahlnknoten. Nach dem Auflegen wird der Originalzustand wieder hergestellt.

- remote ip

```
ISDN_CIRC_%_REMOTE='ip address/netmaskbits'
ISDN_CIRC_%_ROUTE='network/netmaskbits'
```

Beim Konfigurieren des Interfaces erscheinen Routen in das Zielnetz (entsprechend ip-adress AND netmask). Wird die spezifizierte IP nach dem Einwählen beibehalten (dass heißt, es wird keine andere ip während des Verbindungsaufbaus ausgehandelt), bleibt die Route bestehen.

Wird allerdings beim Einwählen eine andere IP ausgehandelt, ändert sich die Route entsprechend (new ip AND netmask).

Für die zusätzlichen Routen gilt das oben gesagte.

Das löst hoffentlich vorläufig *alle* Probleme, die mit speziellen Routen auftraten. Die Form der Korrektur mag sich in Zukunft noch ändern, an dem Prinzip ändert sich hoffentlich nichts mehr.

### B.11.2. Fehlermeldungen des ISDN-Subsystems (englisch, i4l-Dokumentation)

Im folgenden ein Auszug aus der Isdn4Linux Dokumentation (man 7 isdn\_cause).

Cause messages are 2-byte information elements, describing the state transitions of an ISDN line. Each cause message describes its origination (location) in one byte, while the cause code is described in the other byte. Internally, when EDSS1 is used, the first byte contains the location while the second byte contains the cause code. When using 1TR6, the first byte contains the cause code while the location is coded in the second byte. In the Linux ISDN subsystem, the cause messages visible to the user are unified to avoid confusion. All user visible cause messages are displayed as hexadecimal strings. These strings always have the location coded in the first byte, regardless if using 1TR6 or EDSS1. When using EDSS1, these strings are preceded by the character 'E'.

**LOCATION** The following location codes are defined when using EDSS1:

- 00 Message generated by user.
- 01 Message generated by private network serving the local user.
- 02 Message generated by public network serving the local user.
- 03 Message generated by transit network.

## *B. Anhänge der optionalen Pakete*

- 04 Message generated by public network serving the remote user.
- 05 Message generated by private network serving the remote user.
- 07 Message generated by international network.
- 0A Message generated by network beyond inter-working point.

**CAUSE** The following cause codes are defined when using EDSS1:

- 01 Unallocated (unassigned) number.
- 02 No route to specified transit network.
- 03 No route to destination.
- 06 Channel unacceptable.
- 07 Call awarded and being delivered in an established channel.
- 10 Normal call clearing.
- 11 User busy.
- 12 No user responding.
- 13 No answer from user (user alerted).
- 15 Call rejected.
- 16 Number changed.
- 1A Non-selected user clearing.
- 1B Destination out of order.
- 1C Invalid number format.
- 1D Facility rejected.
- 1E Response to status enquiry.
- 1F Normal, unspecified.
- 22 No circuit or channel available.
- 26 Network out of order.
- 29 Temporary failure.
- 2A Switching equipment congestion.
- 2B Access information discarded.
- 2C Requested circuit or channel not available.
- 2F Resources unavailable, unspecified.
- 31 Quality of service unavailable.
- 32 Requested facility not subscribed.
- 39 Bearer capability not authorised.
- 3A Bearer capability not presently available.
- 3F Service or option not available, unspecified.
- 41 Bearer capability not implemented.
- 42 Channel type not implemented.
- 45 Requested facility not implemented.
- 46 Only restricted digital information bearer.
- 4F Service or option not implemented, unspecified.
- 51 Invalid call reference value.
- 52 Identified channel does not exist.
- 53 A suspended call exists, but this call identity does not.
- 54 Call identity in use.
- 55 No call suspended.
- 56 Call having the requested call identity.
- 58 Incompatible destination.
- 5B Invalid transit network selection.
- 5F Invalid message, unspecified.
- 60 Mandatory information element is missing.
- 61 Message type non-existent or not implemented.

- 62 Message not compatible with call state or message or message type non existent or not implemented.
- 63 Information element non-existent or not implemented.
- 64 Invalid information element content.
- 65 Message not compatible.
- 66 Recovery on timer expiry.
- 6F Protocol error, unspecified.
- 7F Inter working, unspecified.

## B.12. UMTS

### B.12.1. Unterstützte Hardware

Dieses Paket unterstützt die im Folgenden gelistete UMTS-Hardware. Für den Betrieb sind unter anderem auch weitere Pakete erforderlich. Für USB-Adapter muss das USB-Paket via OPT\_USB='yes' aktiviert werden.

Hardware:	getestet	zusätzliche Pakete
Novatel Adapter:		
Merlin U530	ja	PCMCIA, TOOLS (serial)
Merlin U630	nein	PCMCIA, TOOLS (serial)
MC950D	ja	USB
OPTION Adapter:		
3G Datacard	nein	PCMCIA, USB
GT 3G Quad	ja	PCMCIA, USB
GT Fusion	nein	PCMCIA, USB
GT MAX HSUPA GX0301	ja	PCMCIA, USB

(bei den vier Cardbusadaptern ist PCMCIA\_PCIC='yenta\_socket' zu setzen)

Icon 225 (GI0225)	ja	USB
Huawei Adapter:		
E220, E230, E270	ja	USB
E510	ja	USB
E800	ja	USB
K3520	ja	USB
ZTE Adapter:		
MF110	ja	USB
MF190	ja	USB

Karten von verschiedenen Herstellern basierend auf den Chipsätzen:

GOBI 1000	ja	USB
-----------	----	-----

GOBI 2000

ja

USB

Es werden zusätzlich die entsprechende Firmwaredateien im Verzeichnis `<config-dir>/lib/firmware/gobi/` benötigt. Wie man diese findet und bereitstellt kann über eine Suchmaschine festgestellt werden: Begriffe `gobi_loader`, `firmware`

### B.12.2. Modemschnittstelle nicht aktiviert

Bei einigen UMTS-Sticks des Typs OPTION kann es vorkommen, dass die Modemschnittstelle nicht aktiviert ist, welche aber für den PPP-Dämon benötigt wird.

### B.12.3. Beispiel

Es folgt ein Beispiel anhand eines GIO225 Adapters. Zuerst werden die verfügbaren Schnittstellen geprüft:

```
grep "" /sys/bus/usb/devices/*/tty*/hsotype
```

Die Ausgabe sollte etwa so aussehen:

```
/sys/bus/usb/devices/2-1:1.0/tty/ttyHS0/hsotype:Control
/sys/bus/usb/devices/2-1:1.0/tty/ttyHS1/hsotype:Application
/sys/bus/usb/devices/2-1:1.1/tty/ttyHS2/hsotype:Diagnostic
```

Hier fehlt die Ausgabe `hsotype:Modem`.

Jetzt kann man mit dem folgenden Befehl die Interface-Konfiguration abfragen:

```
chat -e -t 1 '' "AT_OIFC?" OK >/dev/ttyHS0 </dev/ttyHS0
```

Die Ausgabe sollte folgendermassen aussehen:

```
AT_OIFC?
_OIFC: 3,1,1,0
```

OK

Sollte dort Folgendes stehen:

```
AT_OIFC?
_OIFC: 2,1,1,0
```

OK

kann man die Modemschnittstelle mit dem folgenden Befehl aktivieren:

```
chat -e -t 1 '' "AT_OIFC=3,1,1,0" OK >/dev/ttyHS0 </dev/ttyHS0
```

Danach den Adapter noch einmal abziehen und neu anstecken. Jetzt sollte mittels

```
grep "" /sys/bus/usb/devices/*/tty*/hsotype
```

auch ein Modemeintrag vorhanden sein:

```
/sys/bus/usb/devices/2-1:1.0/tty/ttyHS0/hsotype:Control
/sys/bus/usb/devices/2-1:1.0/tty/ttyHS1/hsotype:Application
/sys/bus/usb/devices/2-1:1.1/tty/ttyHS2/hsotype:Diagnostic
/sys/bus/usb/devices/2-1:1.2/tty/ttyHS3/hsotype:Modem
```



## B.13. Unterschiede Version 4.0.0 und 3.6.2

### Package ADVANCED\_NETWORKING

#### Neue Variablen

[BCRELAY\\_N](#) (Seite 113)  
[BCRELAY\\_x\\_IF\\_N](#) (Seite 113)  
[BCRELAY\\_x\\_IF\\_x](#) (Seite 113)  
[DSA\\_N](#) (Seite ??)  
[DSA\\_x\\_BRIDGE](#) (Seite ??)  
[DSA\\_x\\_DEV](#) (Seite ??)  
[DSA\\_x\\_GROUP\\_N](#) (Seite ??)  
[DSA\\_x\\_GROUP\\_x\\_PORT\\_N](#) (Seite ??)  
[DSA\\_x\\_GROUP\\_x\\_PORT\\_x\\_DEV](#) (Seite ??)  
[ETHTOOL\\_DEV\\_N](#) (Seite 126)  
[ETHTOOL\\_DEV\\_x](#) (Seite 126)  
[ETHTOOL\\_DEV\\_x\\_OPTION\\_N](#) (Seite 126)  
[ETHTOOL\\_DEV\\_x\\_OPTION\\_x\\_NAME](#) (Seite 126)  
[ETHTOOL\\_DEV\\_x\\_OPTION\\_x\\_VALUE](#) (Seite 126)  
[OPT\\_BCRELAY](#) (Seite 113)  
[OPT\\_DSA](#) (Seite ??)  
[OPT\\_ETHTOOL](#) (Seite 126)  
[OPT\\_IPSET](#) (Seite ??)  
[OPT\\_SWITCH](#) (Seite 124)  
[SWITCH\\_N](#) (Seite 124)  
[SWITCH\\_x\\_DEV](#) (Seite 124)  
[SWITCH\\_x\\_VLAN\\_N](#) (Seite 124)  
[SWITCH\\_x\\_VLAN\\_x\\_ID](#) (Seite ??)  
[SWITCH\\_x\\_VLAN\\_x\\_PORT\\_N](#) (Seite ??)  
[SWITCH\\_x\\_VLAN\\_x\\_PORT\\_x\\_ID](#) (Seite ??)  
[SWITCH\\_x\\_VLAN\\_x\\_PORT\\_x\\_MODE](#) (Seite ??)

#### Gelöschte Variablen

### Package BASE

#### Neue Variablen

[ARCH](#) (Seite ??)  
[COMP\\_TYPE\\_ROOTFS](#) (Seite 32)  
[DEBUG\\_IPTABLES](#) (Seite 37)  
[FLI4L\\_BUILDDATE](#) (Seite ??)  
[FLI4L\\_BUILDDIR](#) (Seite ??)  
[FLI4L\\_BUILDTIME](#) (Seite ??)  
[FLI4L\\_VERSION](#) (Seite ??)  
[HOSTNAME\\_IP6](#) (Seite 45)  
[IPV6\\_NET\\_x](#) (Seite 45)  
[IPV6\\_NET\\_x\\_ADVERTISE](#) (Seite 46)  
[IPV6\\_NET\\_x\\_ADVERTISE\\_DNS](#) (Seite 46)  
[IPV6\\_NET\\_x\\_ADVERTISE\\_PREF\\_LIFETIME](#)  
(Seite ??)  
[IPV6\\_NET\\_x\\_ADVERTISE\\_VALID\\_LIFETIME](#)  
(Seite ??)  
[IPV6\\_NET\\_x\\_DEV](#) (Seite 46)  
[IPV6\\_NET\\_x\\_NAME](#) (Seite 46)  
[IPV6\\_ROUTE\\_x](#) (Seite 49)  
[LIBATA\\_DMA](#) (Seite 30)  
[LUATESTS\\_RUNATBOOTTIME](#) (Seite ??)  
[LUA\\_VERSION](#) (Seite ??)  
[NET\\_PREFIX\\_ULA\\_SAVEDIR](#) (Seite ??)

#### Gelöschte Variablen

[COMPRESS\\_KERNEL](#)  
[COMPRESS\\_OPT](#)  
[COMPRESS\\_ROOTFS](#)  
[DENY\\_ICMP](#)  
[DIALMODE](#)  
[DMZ\\_LOG](#)  
[DMZ\\_NAT](#)  
[DMZ\\_ORANGE\\_RED\\_N](#)  
[DMZ\\_ORANGE\\_RED\\_x](#)  
[DMZ\\_ORANGE\\_ROUTER\\_N](#)  
[DMZ\\_ORANGE\\_ROUTER\\_x](#)  
[DMZ\\_RED\\_DEV](#)  
[FORWARD\\_DENY\\_PORT\\_N](#)  
[FORWARD\\_DENY\\_PORT\\_x](#)  
[FORWARD\\_HOST\\_N](#)  
[FORWARD\\_HOST\\_WHITE](#)  
[FORWARD\\_HOST\\_x](#)  
[HOSTNAME\\_ALIAS\\_N](#)  
[IMOND\\_ADMIN\\_PASS](#)  
[IMOND\\_BEEP](#)

## B. Anhänge der optionalen Pakete

NET\_PREFIX\_x\_NAME (Seite 47)  
NET\_PREFIX\_x\_STATIC\_IPV4 (Seite 47)  
NET\_PREFIX\_x\_STATIC\_IPV6 (Seite 47)  
NET\_PREFIX\_x\_TYPE (Seite 47)  
NET\_PREFIX\_x\_ULA\_DEV (Seite 48)  
OPT\_BASE (Seite ??)  
OPT\_HOTPLUG\_PCI (Seite 110)  
OPT\_IPV4 (Seite 41)  
OPT\_IPV6 (Seite 45)  
OPT\_LUA (Seite ??)  
OPT\_LUATESTS (Seite ??)  
OPT\_NET\_PREFIX (Seite 46)  
OPT\_NET\_PREFIX\_ULA (Seite ??)  
PF6\_DNS\_EXCEPTIONS (Seite ??)  
PF6\_FORWARD\_ACCEPT\_DEF (Seite 79)  
PF6\_FORWARD\_LOG (Seite 79)  
PF6\_FORWARD\_LOG\_LIMIT (Seite 79)  
PF6\_FORWARD\_POLICY (Seite 78)  
PF6\_FORWARD\_REJ\_LIMIT (Seite 79)  
PF6\_FORWARD\_UDP\_REJ\_LIMIT (Seite 79)  
PF6\_FORWARD\_x (Seite 79)  
PF6\_FORWARD\_x\_COMMENT (Seite 80)  
PF6\_INPUT\_ACCEPT\_DEF (Seite 77)  
PF6\_INPUT\_ICMP\_ECHO\_REQ\_LIMIT (Seite ??)  
PF6\_INPUT\_ICMP\_ECHO\_REQ\_SIZE (Seite 78)  
PF6\_INPUT\_LOG (Seite 77)  
PF6\_INPUT\_LOG\_LIMIT (Seite 77)  
PF6\_INPUT\_POLICY (Seite 77)  
PF6\_INPUT\_REJ\_LIMIT (Seite 77)  
PF6\_INPUT\_UDP\_REJ\_LIMIT (Seite 77)  
PF6\_INPUT\_x (Seite 78)  
PF6\_INPUT\_x\_COMMENT (Seite 78)  
PF6\_LOG\_LEVEL (Seite 77)  
PF6\_OUTPUT\_ACCEPT\_DEF (Seite 80)  
PF6\_OUTPUT\_CT\_ACCEPT\_DEF (Seite ??)  
PF6\_OUTPUT\_CT\_x (Seite ??)  
PF6\_OUTPUT\_CT\_x\_COMMENT (Seite ??)  
PF6\_OUTPUT\_LOG (Seite 80)  
PF6\_OUTPUT\_LOG\_LIMIT (Seite 80)  
PF6\_OUTPUT\_POLICY (Seite 80)  
PF6\_OUTPUT\_REJ\_LIMIT (Seite 80)  
PF6\_OUTPUT\_UDP\_REJ\_LIMIT (Seite 80)  
PF6\_OUTPUT\_x (Seite 81)  
PF6\_OUTPUT\_x\_COMMENT (Seite 81)  
PF6\_POSTROUTING\_x (Seite 82)  
PF6\_POSTROUTING\_x\_COMMENT (Seite 82)  
PF6\_PREROUTING\_CT\_ACCEPT\_DEF (Seite ??)  
PF6\_PREROUTING\_CT\_x (Seite ??)  
PF6\_PREROUTING\_CT\_x\_COMMENT (Seite ??)  
PF6\_PREROUTING\_x (Seite 82)  
PF6\_PREROUTING\_x\_COMMENT (Seite 82)  
PF6\_USR\_CHAIN\_x\_NAME (Seite 81)  
PF6\_USR\_CHAIN\_x\_RULE\_x (Seite 81)  
PF6\_USR\_CHAIN\_x\_RULE\_x\_COMMENT (Seite 82)  
PF\_DNS\_EXCEPTIONS (Seite ??)  
PF\_INPUT\_ICMP\_ECHO\_REQ\_SIZE (Seite 61)  
PF\_OUTPUT\_ACCEPT\_DEF (Seite 63)  
PF\_OUTPUT\_CT\_ACCEPT\_DEF (Seite 76)  
PF\_OUTPUT\_CT\_x (Seite 76)  
PF\_OUTPUT\_CT\_x\_COMMENT (Seite 76)  
PF\_OUTPUT\_LOG (Seite 63)  
PF\_OUTPUT\_LOG\_LIMIT (Seite 64)  
PF\_OUTPUT\_POLICY (Seite 63)  
PF\_OUTPUT\_REJ\_LIMIT (Seite 64)  
PF\_OUTPUT\_UDP\_REJ\_LIMIT (Seite 64)  
PF\_OUTPUT\_x (Seite 64)  
IMOND\_DIAL  
IMOND\_ENABLE  
IMOND\_LED  
IMOND\_LOG  
IMOND\_LOGDIR  
IMOND\_PASS  
IMOND\_PORT  
IMOND\_REBOOT  
IMOND\_ROUTE  
IMOND\_USE\_ORIG  
INPUT\_ACCEPT\_PORT\_N  
INPUT\_ACCEPT\_PORT\_x  
INPUT\_POLICY  
IP\_DYN\_ADDR  
IP\_NET\_N  
IP\_NET\_x\_TYPE  
IP\_ROUTE\_N  
LIBC\_VERSION  
MASQ\_MODULE\_N  
MASQ\_NETWORK  
NET\_DRV\_N  
OPT\_DMZ  
OPT\_EVSS  
OPT\_MOUNTFLOPPY  
PACKETFILTER\_LOG  
PACKETFILTER\_LOG\_LEVEL  
PF\_FORWARD\_N  
PF\_INPUT\_N  
PF\_NEW\_CONFIG  
PF\_POSTROUTING\_N  
PF\_PREROUTING\_N  
PF\_USR\_CHAIN\_N  
PF\_USR\_CHAIN\_x\_RULE\_N  
PORTFW\_N  
PRESERVE  
ROUTE\_NETWORK  
START\_IMOND  
SYSLOGD\_DEST\_N  
TRUSTED\_NETS

PF\_OUTPUT\_x\_COMMENT (Seite 64)  
 PF\_PREROUTING\_CT\_ACCEPT\_DEF (Seite 76)  
 PF\_PREROUTING\_CT\_x (Seite 76)  
 PF\_PREROUTING\_CT\_x\_COMMENT (Seite 76)  
 RTC\_SYNC (Seite 31)  
 SYSLOGD\_ROTATE\_AT\_SHUTDOWN (Seite 107)

## Package CIRCUITS

### Neue Variablen

CIRC\_CLASS\_x\_NAME (Seite 97)  
 CIRC\_ONLINE (Seite 102)  
 CIRC\_x\_BUNDLE (Seite 93)  
 CIRC\_x\_CHARGEINT (Seite 91)  
 CIRC\_x\_CLASS\_x (Seite ??)  
 CIRC\_x\_DEBUG (Seite 92)  
 CIRC\_x\_DEPS (Seite 92)  
 CIRC\_x\_DIALMODE (Seite 88)  
 CIRC\_x\_ENABLED (Seite 88)  
 CIRC\_x\_HUP\_TIMEOUT (Seite 91)  
 CIRC\_x\_NAME (Seite 87)  
 CIRC\_x\_NETS\_IPV4\_x (Seite ??)  
 CIRC\_x\_NETS\_IPV4\_x\_GATEWAY (Seite ??)  
 CIRC\_x\_NETS\_IPV6\_x (Seite ??)  
 CIRC\_x\_NETS\_IPV6\_x\_GATEWAY (Seite ??)  
 CIRC\_x\_NET\_IF (Seite ??)  
 CIRC\_x\_NET\_IPV4\_ADDRESS (Seite ??)  
 CIRC\_x\_NET\_IPV6\_ADDRESS (Seite ??)  
 CIRC\_x\_NET\_IPV6\_ADVERTISE\_PREFIX (Seite ??)  
 CIRC\_x\_NET\_IPV6\_ADVERTISE\_PREFIX\_ON\_LINK (Seite ??)  
 CIRC\_x\_NET\_IPV6\_ADVERTISE\_PREFIX\_PREFERRED\_LIFETIME (Seite ??)  
 CIRC\_x\_NET\_IPV6\_ADVERTISE\_PREFIX\_VALID\_LIFETIME (Seite ??)  
 CIRC\_x\_PRIORITY (Seite 89)  
 CIRC\_x\_PROTOCOLS (Seite 89)  
 CIRC\_x\_REDIAL\_DELAY (Seite ??)  
 CIRC\_x\_ROUTE\_DEV (Seite 103)  
 CIRC\_x\_ROUTE\_GATEWAY\_IPV4 (Seite 103)  
 CIRC\_x\_ROUTE\_GATEWAY\_IPV6 (Seite 104)  
 CIRC\_x\_TIMES (Seite 90)  
 CIRC\_x\_TYPE (Seite 88)  
 CIRC\_x\_UP (Seite 89)  
 CIRC\_x\_USEPEERDNS (Seite 91)  
 CIRC\_x\_WAIT (Seite 92)  
 OPT\_BUNDLE (Seite ??)  
 OPT\_CIRCUIT\_STATUS (Seite 103)  
 OPT\_IMOND (Seite 83)  
 OPT\_NET (Seite ??)

### Gelöschte Variablen

ADDMODULES  
 BEEP  
 BOOTMENU\_TIME  
 BOOT\_TYPE  
 BUG\_CHECK  
 COMPRESS\_KERNEL  
 COMPRESS\_OPT  
 COMPRESS\_ROOTFS  
 COMP\_TYPE\_OPT  
 CONSOLE\_BLANK\_TIME  
 DEBUG\_ENABLE\_CORE  
 DEBUG\_IP  
 DEBUG\_IPUP  
 DEBUG\_KEEP\_BOOTLOGD  
 DEBUG\_MDEV  
 DEBUG\_MODULES  
 DEBUG\_STARTUP  
 DENY\_ICMP  
 DMZ\_LOG  
 DMZ\_NAT  
  
 DMZ\_ORANGE\_RED\_N  
  
 DMZ\_ORANGE\_RED\_x  
  
 DMZ\_ORANGE\_ROUTER\_N  
 DMZ\_ORANGE\_ROUTER\_x  
 DMZ\_RED\_DEV  
 DNS\_FORWARDERS  
 DOMAIN\_NAME  
 FLI4L\_UUID  
 FORWARD\_DENY\_PORT\_N  
 FORWARD\_DENY\_PORT\_x  
 FORWARD\_HOST\_N  
 FORWARD\_HOST\_WHITE  
 FORWARD\_HOST\_x  
 HOSTNAME  
 HOSTNAME\_ALIAS\_N  
 HOSTNAME\_ALIAS\_x  
 HOSTNAME\_IP  
 IGNORE\_IP\_NET\_WARNING  
 IMOND\_USE\_ORIG  
 INPUT\_ACCEPT\_PORT\_N  
 INPUT\_ACCEPT\_PORT\_x  
 INPUT\_POLICY  
 IP\_CONNTRACK\_MAX  
 IP\_NET\_N  
 IP\_NET\_x  
 IP\_NET\_x\_COMMENT  
 IP\_NET\_x\_DEV  
 IP\_NET\_x\_MAC  
 IP\_NET\_x\_NAME

## B. Anhänge der optionalen Pakete

IP\_NET\_x\_TYPE  
IP\_ROUTE\_N  
IP\_ROUTE\_x  
KERNEL\_BOOT\_OPTION  
KERNEL\_VERSION  
KEYBOARD\_LOCALE  
LIBC\_VERSION  
LOCALE  
LOGIP\_LOGDIR  
LOG\_BOOT\_SEQ  
MASQ\_MODULE\_N  
MASQ\_MODULE\_x  
MASQ\_MODULE\_x\_OPTION  
MASQ\_NETWORK  
MOUNT\_BOOT  
NET\_DRV\_N  
NET\_DRV\_x  
NET\_DRV\_x\_OPTION  
OPT\_ADDMODULES  
OPT\_DMZ  
OPT\_EVSS  
OPT\_KLOGD  
OPT\_LOGIP  
OPT\_MAKEKBL  
OPT\_MOUNTFLOPPY  
OPT\_PNP  
OPT\_SYSLOGD  
OPT\_Y2K  
PACKETFILTER\_LOG  
PACKETFILTER\_LOG\_LEVEL  
PASSWORD  
PF\_FORWARD\_ACCEPT\_DEF  
PF\_FORWARD\_LOG  
PF\_FORWARD\_LOG\_LIMIT  
PF\_FORWARD\_N  
PF\_FORWARD\_POLICY  
PF\_FORWARD\_REJ\_LIMIT  
PF\_FORWARD\_UDP\_REJ\_LIMIT  
PF\_FORWARD\_x  
PF\_FORWARD\_x\_COMMENT  
PF\_INPUT\_ACCEPT\_DEF  
PF\_INPUT\_ICMP\_ECHO\_REQ\_LIMIT  
PF\_INPUT\_LOG  
PF\_INPUT\_LOG\_LIMIT  
PF\_INPUT\_N  
PF\_INPUT\_POLICY  
PF\_INPUT\_REJ\_LIMIT  
PF\_INPUT\_UDP\_REJ\_LIMIT  
PF\_INPUT\_x  
PF\_INPUT\_x\_COMMENT  
PF\_LOG\_LEVEL  
PF\_NEW\_CONFIG  
PF\_POSTROUTING\_N  
PF\_POSTROUTING\_x  
PF\_POSTROUTING\_x\_COMMENT  
PF\_PREROUTING\_N  
PF\_PREROUTING\_x  
PF\_PREROUTING\_x\_COMMENT  
PF\_USR\_CHAIN\_N  
PF\_USR\_CHAIN\_x\_NAME  
PF\_USR\_CHAIN\_x\_RULE\_N  
PF\_USR\_CHAIN\_x\_RULE\_x  
PF\_USR\_CHAIN\_x\_RULE\_x\_COMMENT  
PORTFW\_N  
PORTFW\_x\_COMMENT  
PORTFW\_x\_NEW\_TARGET

## B. Anhänge der optionalen Pakete

PORTFW\_x\_PROTOCOL  
PORTFW\_x\_TARGET  
POWERMANAGEMENT  
PRESERVE  
ROUTE\_NETWORK  
SER\_CONSOLE  
SER\_CONSOLE\_IF  
SER\_CONSOLE\_RATE  
START\_IMOND  
SYSLOGD\_DEST\_N  
SYSLOGD\_DEST\_x  
SYSLOGD\_RECEIVER  
SYSLOGD\_ROTATE  
SYSLOGD\_ROTATE\_DIR  
SYSLOGD\_ROTATE\_MAX  
TIME\_INFO  
TRUSTED\_NETS  
Y2K\_DAYS

### Package CERT

#### Neue Variablen

[CERT\\_X509\\_MOZILLA](#) (Seite 128)  
[OPT\\_CERT](#) (Seite 128)  
[OPT\\_CERT\\_X509](#) (Seite 128)

#### Gelöschte Variablen

### Package CHRONY

#### Neue Variablen

#### Gelöschte Variablen

CHRONY\_BIOS\_TIME

### Package DNS\_DHCP

#### Neue Variablen

#### Gelöschte Variablen

[CIRC\\_x\\_DHCP\\_ACCEPT\\_CSR](#) (Seite 145)  
[CIRC\\_x\\_DHCP\\_DAEMON](#) (Seite 144)  
[CIRC\\_x\\_DHCP\\_DEV](#) (Seite 144)  
[CIRC\\_x\\_DHCP\\_HOSTNAME](#) (Seite 144)  
[CIRC\\_x\\_DHCP\\_PREFIX\\_LENGTH](#) (Seite ??)  
[CIRC\\_x\\_DHCP\\_SERVER\\_DAEMON](#) (Seite ??)  
[CIRC\\_x\\_DHCP\\_SERVER\\_DEV](#) (Seite ??)  
[CIRC\\_x\\_DHCP\\_SERVER\\_PREFIX\\_POOL\\_N](#) (Seite ??)  
[CIRC\\_x\\_DHCP\\_SERVER\\_PREFIX\\_POOL\\_x-](#)  
[NETWORK](#) (Seite ??)  
[CIRC\\_x\\_DHCP\\_SERVER\\_PREFIX\\_POOL\\_x-](#)  
[PREFIX\\_LENGTH](#) (Seite ??)  
[CIRC\\_x\\_DHCP\\_STARTDELAY](#) (Seite 144)  
[CIRC\\_x\\_NET\\_IPV6\\_ADVERTISE\\_DNS](#) (Seite ??)  
[DHCP\\_DNS\\_SERVERS](#) (Seite 139)  
[DHCP\\_EXTRA\\_RANGE\\_x\\_DNS\\_SERVERS](#) (Seite 141)  
[DHCP\\_EXTRA\\_RANGE\\_x\\_NTP\\_SERVERS](#) (Seite 141)  
[DHCP\\_EXTRA\\_RANGE\\_x\\_WINS\\_SERVERS](#) (Seite 141)  
[DHCP\\_NTP\\_SERVERS](#) (Seite 139)  
[DHCP\\_OPTION\\_WPAD](#) (Seite 139)

DHCPRELAY\_IF\_N  
DHCP\_DENY\_MAC\_N  
DHCP\_EXTRA\_RANGE\_N  
DHCP\_EXTRA\_RANGE\_x\_DNS\_SERVER  
DHCP\_EXTRA\_RANGE\_x\_NTP\_SERVER  
DHCP\_RANGE\_N  
DHCP\_RANGE\_x\_DNS\_SERVER1  
DHCP\_RANGE\_x\_DNS\_SERVER2  
DHCP\_RANGE\_x\_NTP\_SERVER  
  
DHCP\_RANGE\_x\_OPTION\_N  
  
DHCP\_WINSERVER\_1  
DHCP\_WINSERVER\_2  
DNS\_FORBIDDEN\_N  
DNS\_LISTENIP\_N  
DNS\_LISTENIP\_x  
DNS\_REBINDOK\_N  
DNS\_REDIRECT\_N  
DNS\_SPECIAL\_N

## B. Anhänge der optionalen Pakete

<a href="#">DHCP_OPTION_WPAD_URL</a> (Seite 140)	<a href="#">DNS_SPECIAL_x_DNSIP</a>
<a href="#">DHCP_RANGE_x_DNS_SERVERS</a> (Seite 140)	<a href="#">DNS_SPECIAL_x_DOMAIN</a>
<a href="#">DHCP_RANGE_x_NTP_SERVERS</a> (Seite 140)	<a href="#">DNS_SPECIAL_x_NETWORK</a>
<a href="#">DHCP_RANGE_x_OPTION_WPAD</a> (Seite 140)	<a href="#">HOST_EXTRA_N</a>
<a href="#">DHCP_RANGE_x_OPTION_WPAD_URL</a> (Seite 141)	<a href="#">HOST_N</a>
<a href="#">DHCP_RANGE_x_WINS_SERVERS</a> (Seite 140)	<a href="#">HOST_x_ALIAS_N</a>
<a href="#">DHCP_SERVER_LEASES_DIR</a> (Seite ??)	
<a href="#">DHCP_WINS_SERVERS</a> (Seite 139)	
<a href="#">DNS_AUTHORITATIVE</a> (Seite 135)	
<a href="#">DNS_AUTHORITATIVE_LISTEN</a> (Seite 136)	
<a href="#">DNS_AUTHORITATIVE_NS</a> (Seite 136)	
<a href="#">DNS_BIND_INTERFACES</a> (Seite 133)	
<a href="#">DNS_FORWARD_LOCAL</a> (Seite ??)	
<a href="#">DNS_FORWARD_PRIV_x</a> (Seite 134)	
<a href="#">DNS_LISTEN_x</a> (Seite 132)	
<a href="#">DNS_LOCAL_HOST_CACHE_TTL</a> (Seite 135)	
<a href="#">DNS_ZONE_DELEGATION_x_DOMAIN_x</a> (Seite ??)	
<a href="#">DNS_ZONE_DELEGATION_x_NETWORK_x</a> (Seite ??)	
<a href="#">DNS_ZONE_DELEGATION_x_UPSTREAM_SERVER_x_IP</a> (Seite ??)	
<a href="#">DNS_ZONE_DELEGATION_x_UPSTREAM_SERVER_x_QUERYSOURCEIP</a> (Seite ??)	
<a href="#">DNS_ZONE_NETWORK_x</a> (Seite 136)	
<a href="#">HOST_x_IP6_NET</a> (Seite ??)	
<a href="#">OPT_DHCP_CLIENT</a> (Seite 143)	
<a href="#">OPT_DHCP_SERVER</a> (Seite ??)	
<a href="#">OPT_YADIFA</a> (Seite ??)	
<a href="#">YADIFA_ALLOW_QUERY_x</a> (Seite ??)	
<a href="#">YADIFA_LISTEN_x</a> (Seite ??)	
<a href="#">YADIFA_SLAVE_ZONE_x</a> (Seite 148)	
<a href="#">YADIFA_SLAVE_ZONE_x_ALLOW_QUERY_x</a> (Seite 148)	
<a href="#">YADIFA_SLAVE_ZONE_x_MASTER</a> (Seite 148)	
<a href="#">YADIFA_SLAVE_ZONE_x_USE_DNSMASQ_ZONE_DELEGATION</a> (Seite ??)	
<a href="#">YADIFA_USE_DNSMASQ_ZONE_DELEGATION</a> (Seite ??)	

## Package DYNDNS

### Neue Variablen

[DYNDNS\\_x\\_CHECK\\_TIME](#) (Seite ??)  
[DYNDNS\\_x\\_CHECK\\_WITH](#) (Seite ??)  
[DYNDNS\\_x\\_CIRCUIT\\_N](#) (Seite ??)  
[DYNDNS\\_x\\_CIRCUIT\\_x](#) (Seite ??)  
[DYNDNS\\_x\\_DETECT\\_EXT\\_IPV4](#) (Seite ??)  
[DYNDNS\\_x\\_DETECT\\_EXT\\_IPV6](#) (Seite ??)  
[DYNDNS\\_x\\_FORCE\\_UPDATE\\_TIME](#) (Seite ??)  
[DYNDNS\\_x\\_LOGIN\\_PASSWORD](#) (Seite ??)  
[DYNDNS\\_x\\_LOGIN\\_TIME](#) (Seite ??)  
[DYNDNS\\_x\\_LOGIN\\_USERNAME](#) (Seite ??)  
[DYNDNS\\_x\\_UPDATE\\_A](#) (Seite ??)  
[DYNDNS\\_x\\_UPDATE\\_AAAA](#) (Seite ??)  
[DYNDNS\\_x\\_UPDATE\\_AAAA\\_TTL](#) (Seite ??)  
[DYNDNS\\_x\\_UPDATE\\_A\\_TTL](#) (Seite ??)  
[DYNDNS\\_x\\_UPDATE\\_HOST\\_N](#) (Seite ??)  
[DYNDNS\\_x\\_UPDATE\\_HOST\\_x](#) (Seite ??)  
[DYNDNS\\_x\\_UPDATE\\_HOST\\_x\\_CA](#) (Seite ??)  
[DYNDNS\\_x\\_UPDATE\\_MX](#) (Seite ??)  
[DYNDNS\\_x\\_UPDATE\\_MX\\_TTL](#) (Seite ??)  
[DYNDNS\\_x\\_UPDATE\\_WILDCARD](#) (Seite ??)  
[DYNDNS\\_x\\_UPDATE\\_WILDCARD\\_TTL](#) (Seite ??)

### Gelöschte Variablen

[DYNDNS\\_ALLOW\\_SSL](#)  
[DYNDNS\\_x\\_CIRCUIT](#)  
[DYNDNS\\_x\\_EXT\\_IP](#)  
[DYNDNS\\_x\\_RENEW](#)  
[DYNDNS\\_x\\_UPDATEHOST](#)  
[DYNDNS\\_x\\_USER](#)

DYNDNS\_x\_USERNAME (Seite ??)  
[OPT\\_STUN](#) (Seite 156)  
[STUN\\_SERVER\\_N](#) (Seite 156)  
STUN\_SERVER\_RANDOM (Seite ??)  
[STUN\\_SERVER\\_x](#) (Seite 156)

## Package HD

### Neue Variablen

[AUTOMOUNT\\_UNKNOWN](#) (Seite 162)  
[AUTOMOUNT\\_UNKNOWN\\_OPTS](#) (Seite 162)  
[EXTMOUNT\\_x\\_HOTPLUG](#) (Seite 161)  
[OPT\\_AUTOMOUNT](#) (Seite 162)

### Gelöschte Variablen

HDIT\_DATA  
HDIT\_POWEROFF  
HDIT\_SIZES  
OPT\_HDINSTALL\_TEST

## Package HTTPD

### Neue Variablen

[HTTPD\\_ARPING\\_IGNORE\\_N](#) (Seite 166)  
[HTTPD\\_ARPING\\_IGNORE\\_x](#) (Seite 166)

### Gelöschte Variablen

HTTPD\_GUI\_SKIN

## Package IPV6

### Neue Variablen

CIRC\_x\_TUN6IN4\_HE\_LOCALV6 (Seite ??)  
CIRC\_x\_TUN6IN4\_HE\_PASSWORD (Seite ??)  
CIRC\_x\_TUN6IN4\_HE\_PREFIX (Seite ??)  
CIRC\_x\_TUN6IN4\_HE\_REMOTEV6 (Seite ??)  
CIRC\_x\_TUN6IN4\_HE\_TUNNELID (Seite ??)  
CIRC\_x\_TUN6IN4\_HE\_USERID (Seite ??)  
CIRC\_x\_TUN6IN4\_LOCALV4 (Seite ??)  
CIRC\_x\_TUN6IN4\_MTU (Seite ??)  
CIRC\_x\_TUN6IN4\_REMOTEV4 (Seite ??)  
CIRC\_x\_TUN6IN4\_STATIC\_LOCALV6 (Seite ??)  
CIRC\_x\_TUN6IN4\_STATIC\_PREFIX (Seite ??)  
CIRC\_x\_TUN6IN4\_STATIC\_REMOTEV6 (Seite ??)  
CIRC\_x\_TUN6IN4\_TYPE (Seite ??)

### Gelöschte Variablen

HOSTNAME\_IP6  
IPV6\_NET\_N  
IPV6\_NET\_x  
IPV6\_NET\_x\_ADVERTISE  
IPV6\_NET\_x\_ADVERTISE\_DNS  
IPV6\_NET\_x\_DEV  
IPV6\_NET\_x\_DHCP  
IPV6\_NET\_x\_NAME  
IPV6\_NET\_x\_TUNNEL  
IPV6\_ROUTE\_N  
IPV6\_ROUTE\_x  
IPV6\_TUNNEL\_N  
IPV6\_TUNNEL\_x\_DEFAULT  
IPV6\_TUNNEL\_x\_DEV  
IPV6\_TUNNEL\_x\_LOCALV4  
IPV6\_TUNNEL\_x\_LOCALV6  
IPV6\_TUNNEL\_x\_MTU  
IPV6\_TUNNEL\_x\_PASSWORD  
IPV6\_TUNNEL\_x\_PREFIX  
IPV6\_TUNNEL\_x\_REMOTEV4  
IPV6\_TUNNEL\_x\_REMOTEV6  
IPV6\_TUNNEL\_x\_TIMEOUT  
IPV6\_TUNNEL\_x\_TUNNELID  
IPV6\_TUNNEL\_x\_TYPE  
IPV6\_TUNNEL\_x\_USERID  
OPT\_IPV6  
PF6\_FORWARD\_ACCEPT\_DEF  
PF6\_FORWARD\_LOG  
PF6\_FORWARD\_LOG\_LIMIT  
PF6\_FORWARD\_N  
PF6\_FORWARD\_POLICY

## B. Anhänge der optionalen Pakete

PF6\_FORWARD\_REJ\_LIMIT  
PF6\_FORWARD\_UDP\_REJ\_LIMIT  
PF6\_FORWARD\_x  
PF6\_FORWARD\_x\_COMMENT  
PF6\_INPUT\_ACCEPT\_DEF  
PF6\_INPUT\_LOG  
PF6\_INPUT\_LOG\_LIMIT  
PF6\_INPUT\_N  
PF6\_INPUT\_POLICY  
PF6\_INPUT\_REJ\_LIMIT  
PF6\_INPUT\_UDP\_REJ\_LIMIT  
PF6\_INPUT\_x  
PF6\_INPUT\_x\_COMMENT  
PF6\_USR\_CHAIN\_N  
PF6\_USR\_CHAIN\_x\_NAME  
PF6\_USR\_CHAIN\_x\_RULE\_N  
PF6\_USR\_CHAIN\_x\_RULE\_x  
PF6\_USR\_CHAIN\_x\_RULE\_x\_COMMENT

## Package ISDN

### Neue Variablen

CIRC\_x\_PPP\_ISDN\_DIALOUT (Seite ??)  
CIRC\_x\_PPP\_ISDN\_MSN (Seite ??)  
CIRC\_x\_PPP\_ISDN\_SERVER\_DIALIN (Seite ??)  
CIRC\_x\_PPP\_ISDN\_SERVER\_MSN (Seite ??)  
CIRC\_x\_PPP\_ISDN\_TIMEOUT (Seite ??)  
[ISDN\\_FILTER\\_EXPR \(Seite 183\)](#)  
[ISDN\\_x\\_IO \(Seite 180\)](#)  
[ISDN\\_x\\_IO0 \(Seite 180\)](#)  
[ISDN\\_x\\_IO1 \(Seite 180\)](#)  
[ISDN\\_x\\_IP \(Seite 182\)](#)  
[ISDN\\_x\\_IRQ \(Seite ??\)](#)  
[ISDN\\_x\\_MEM \(Seite 180\)](#)  
[ISDN\\_x\\_PORT \(Seite 182\)](#)  
[ISDN\\_x\\_TYPE \(Seite 180\)](#)  
OPT\_PPP\_ISDN (Seite ??)  
OPT\_PPP\_ISDN\_SERVER (Seite ??)  
[OPT\\_RCAPID \(Seite 195\)](#)  
[RCAPID\\_PORT \(Seite 195\)](#)  
[TELMOND\\_CAPI\\_CTRL\\_N \(Seite 195\)](#)  
[TELMOND\\_CAPI\\_CTRL\\_x \(Seite 195\)](#)

### Gelöschte Variablen

ISDN\_IO  
ISDN\_IO0  
ISDN\_IO1  
ISDN\_IP  
ISDN\_IRQ  
ISDN\_MEM  
ISDN\_PORT  
ISDN\_TYPE

## Package LCD

### Neue Variablen

LCD\_VAR\_TEXT1 (Seite ??)  
LCD\_VAR\_TEXT2 (Seite ??)  
LCD\_VAR\_TEXT3 (Seite ??)  
LCD\_VAR\_TEXT4 (Seite ??)

### Gelöschte Variablen

LCD\_VAR\_TEXT\_1  
LCD\_VAR\_TEXT\_2  
LCD\_VAR\_TEXT\_3  
LCD\_VAR\_TEXT\_4

## Package OPENVPN

### Neue Variablen

### Gelöschte Variablen



## B. Anhänge der optionalen Pakete

OPENVPN_CONVERT_CONF_CON_N (Seite ??)	OPENVPN_DEFAULT_PF_DMZ_TYPE
OPENVPN_CONVERT_CONF_CON_x_FLOAT (Seite ??)	OPENVPN_VERSION
OPENVPN_CONVERT_CONF_CON_x_HOST (Seite ??)	OPENVPN_x_PF_DMZ_TYPE
OPENVPN_CONVERT_CONF_ROUTE_N (Seite ??)	
OPENVPN_CONVERT_CONF_ROUTE_x (Seite ??)	
OPENVPN_DEFAULT_LOCAL_HOST (Seite ??)	
<a href="#">OPENVPN_DEFAULT_RENEG_SEC (Seite 209)</a>	
<a href="#">OPENVPN_x_CHECK_REPLAY (Seite 216)</a>	
OPENVPN_x_IPV6 (Seite ??)	
<a href="#">OPENVPN_x_LOCAL_VPN_IPV6 (Seite 203)</a>	
<a href="#">OPENVPN_x_PF6_FORWARD_N (Seite 215)</a>	
<a href="#">OPENVPN_x_PF6_FORWARD_x (Seite 216)</a>	
<a href="#">OPENVPN_x_PF6_INPUT_N (Seite 215)</a>	
<a href="#">OPENVPN_x_PF6_INPUT_x (Seite 215)</a>	
<a href="#">OPENVPN_x_REMOTE_VPN_IPV6 (Seite 203)</a>	
OPENVPN_x_RENEG_SEC (Seite ??)	
OPT_OPENVPN_CONVERT_CONF (Seite ??)	

## Package PCMCIA

### Neue Variablen

### Gelöschte Variablen

PCMCIA\_CARDMGR\_OPTS  
PCMCIA\_CORE\_OPTS  
PCMCIA\_PCIC\_EXTERN

## Package PPP

### Neue Variablen

### Gelöschte Variablen

<a href="#">CIRC_x_PPP_COMP_BSDCOMP (Seite 231)</a>	PPP_DEV
<a href="#">CIRC_x_PPP_COMP_BSDCOMP_LEVEL (Seite 231)</a>	PPP_IPADDR
<a href="#">CIRC_x_PPP_COMP_DEFLATE (Seite 232)</a>	PPP_NETMASK
<a href="#">CIRC_x_PPP_COMP_DEFLATE_LEVEL (Seite 232)</a>	PPP_NETWORK
<a href="#">CIRC_x_PPP_COMP_LZSCOMP (Seite 232)</a>	PPP_PEER
<a href="#">CIRC_x_PPP_COMP_LZSCOMP_NHIST (Seite 234)</a>	PPP_SPEED
<a href="#">CIRC_x_PPP_COMP_MPPE (Seite 235)</a>	
<a href="#">CIRC_x_PPP_COMP_MPPE_KEY_LEN (Seite 235)</a>	
<a href="#">CIRC_x_PPP_DECOMP_BSDCOMP (Seite 231)</a>	
<a href="#">CIRC_x_PPP_DECOMP_BSDCOMP_LEVEL (Seite 231)</a>	
<a href="#">CIRC_x_PPP_DECOMP_DEFLATE (Seite 232)</a>	
<a href="#">CIRC_x_PPP_DECOMP_DEFLATE_LEVEL (Seite 232)</a>	
<a href="#">CIRC_x_PPP_DECOMP_LZSCOMP (Seite 232)</a>	
<a href="#">CIRC_x_PPP_DECOMP_LZSCOMP_NHIST (Seite 234)</a>	
<a href="#">CIRC_x_PPP_DNS1 (Seite ??)</a>	
<a href="#">CIRC_x_PPP_DNS2 (Seite ??)</a>	
<a href="#">CIRC_x_PPP_FILTER (Seite 228)</a>	
<a href="#">CIRC_x_PPP_FILTER_EXPR (Seite 229)</a>	
<a href="#">CIRC_x_PPP_LCP_ECHO_ADAPTIVE (Seite ??)</a>	
<a href="#">CIRC_x_PPP_LCP_ECHO_INTERVAL (Seite ??)</a>	
<a href="#">CIRC_x_PPP_LCP_ECHO_MAX_FAILURES (Seite ??)</a>	
<a href="#">CIRC_x_PPP_LOCALIP (Seite 228)</a>	
<a href="#">CIRC_x_PPP_LOCALIP6 (Seite 228)</a>	
<a href="#">CIRC_x_PPP_MASTER (Seite 237)</a>	
<a href="#">CIRC_x_PPP_MRRU (Seite 238)</a>	
<a href="#">CIRC_x_PPP_MRU (Seite 227)</a>	
<a href="#">CIRC_x_PPP_MTU (Seite 227)</a>	

[CIRC\\_x\\_PPP\\_NF\\_MSS](#) (Seite 227)  
[CIRC\\_x\\_PPP\\_PASSWORD](#) (Seite 230)  
[CIRC\\_x\\_PPP\\_PEER\\_AUTH](#) (Seite 230)  
[CIRC\\_x\\_PPP\\_REMOTEIP](#) (Seite 228)  
[CIRC\\_x\\_PPP\\_REMOTEIP6](#) (Seite 228)  
[CIRC\\_x\\_PPP\\_SERIAL\\_DEV](#) (Seite 240)  
[CIRC\\_x\\_PPP\\_SERIAL\\_SERVER\\_DEV](#) (Seite 241)  
[CIRC\\_x\\_PPP\\_SERIAL\\_SERVER\\_SPEED](#) (Seite 241)  
[CIRC\\_x\\_PPP\\_SERIAL\\_SPEED](#) (Seite 240)  
[CIRC\\_x\\_PPP\\_TYPE](#) (Seite 227)  
[CIRC\\_x\\_PPP\\_USERID](#) (Seite 229)  
[CIRC\\_x\\_PPP\\_VJ](#) (Seite 230)  
[CIRC\\_x\\_PPP\\_VJCCOMP](#) (Seite 230)  
[CIRC\\_x\\_PPP\\_WINS1](#) (Seite ??)  
[CIRC\\_x\\_PPP\\_WINS2](#) (Seite ??)  
[OPT\\_PPP\\_MULTILINK](#) (Seite ??)  
[OPT\\_PPP\\_PEERS](#) (Seite ??)  
[OPT\\_PPP\\_SERIAL](#) (Seite 240)  
[OPT\\_PPP\\_SERIAL\\_SERVER](#) (Seite 240)  
[PPP\\_COMP\\_LZSCOMP\\_LEVEL](#) (Seite 234)  
[PPP\\_PEER\\_N](#) (Seite ??)  
[PPP\\_PEER\\_x\\_CIRCUITS](#) (Seite ??)  
[PPP\\_PEER\\_x\\_PASSWORD](#) (Seite ??)  
[PPP\\_PEER\\_x\\_REMOTEIPS](#) (Seite ??)  
[PPP\\_PEER\\_x\\_USERID](#) (Seite ??)

## Package PROXY

### Neue Variablen

### Gelöschte Variablen

[IGMPPROXY\\_ALT\\_N](#) (Seite ??)  
[IGMPPROXY\\_ALT\\_x\\_NET](#) (Seite ??)  
[IGMPPROXY\\_DEBUG](#) (Seite ??)  
[IGMPPROXY\\_DEBUG2](#) (Seite ??)  
[IGMPPROXY\\_DOWNLOAD\\_DEV](#) (Seite ??)  
[IGMPPROXY\\_QUICKLEAVE\\_ON](#) (Seite ??)  
[IGMPPROXY\\_UPLOAD\\_DEV](#) (Seite ??)  
[IGMPPROXY\\_WLIST\\_N](#) (Seite ??)  
[IGMPPROXY\\_WLIST\\_x\\_NET](#) (Seite ??)  
[IMPROXY\\_DOWNSTREAM\\_DEV](#) (Seite ??)  
[IMPROXY\\_ENABLE\\_IGMPV3](#) (Seite ??)  
[IMPROXY\\_ENABLE\\_MLD](#) (Seite ??)  
[IMPROXY\\_UPSTREAM\\_DEV](#) (Seite ??)  
[OPT\\_IGMPPROXY](#) (Seite ??)  
[OPT\\_IMPROXY](#) (Seite ??)  
[OPT\\_KAMAILIO](#) (Seite ??)  
[OPT\\_RTTPROXY](#) (Seite ??)  
[OPT\\_SIPROXD](#) (Seite ??)  
[OPT\\_STUNNEL](#) (Seite ??)  
[SIPROXD\\_N](#) (Seite ??)  
[SIPROXD\\_x\\_ALLOW\\_REG\\_N](#) (Seite ??)  
[SIPROXD\\_x\\_ALLOW\\_REG\\_x](#) (Seite ??)  
[SIPROXD\\_x\\_DEV\\_IN](#) (Seite ??)  
[SIPROXD\\_x\\_DEV\\_OUT](#) (Seite ??)  
[SIPROXD\\_x\\_RTP\\_PORT\\_MAX](#) (Seite ??)  
[SIPROXD\\_x\\_RTP\\_PORT\\_MIN](#) (Seite ??)  
[SIPROXD\\_x\\_SIP\\_PORT](#) (Seite ??)  
[SIPROXD\\_x\\_TRANSPARENT](#) (Seite ??)  
[SIPROXD\\_x\\_USER\\_N](#) (Seite ??)  
[SIPROXD\\_x\\_USER\\_x\\_NAME](#) (Seite ??)  
[SIPROXD\\_x\\_USER\\_x\\_PASS](#) (Seite ??)  
[STUNNEL\\_DEBUG](#) (Seite ??)  
[STUNNEL\\_N](#) (Seite ??)

STUNNEL\_x\_ACCEPT (Seite ??)  
STUNNEL\_x\_ACCEPT\_IPV4 (Seite ??)  
STUNNEL\_x\_ACCEPT\_IPV6 (Seite ??)  
STUNNEL\_x\_CERT\_CA\_FILE (Seite ??)  
STUNNEL\_x\_CERT\_FILE (Seite ??)  
STUNNEL\_x\_CERT\_VERIFY (Seite ??)  
STUNNEL\_x\_CLIENT (Seite ??)  
STUNNEL\_x\_CONNECT (Seite ??)  
STUNNEL\_x\_DELAY\_DNS (Seite ??)  
STUNNEL\_x\_NAME (Seite ??)  
STUNNEL\_x\_OUTGOING\_IP (Seite ??)

## Package QOS

### Neue Variablen

[QOS\\_CLASS\\_x\\_LABEL](#) (Seite 249)

### Gelöschte Variablen

## Package SSHD

### Neue Variablen

### Gelöschte Variablen

OPT\_SCP

## Package TOOLS

### Neue Variablen

### Gelöschte Variablen

[FTP\\_PF\\_ENABLE\\_ACTIVE](#) (Seite 267)  
[OPT\\_ATH\\_INFO](#) (Seite 273)  
[OPT\\_BMON](#) (Seite 266)  
[OPT\\_CURL](#) (Seite 266)  
[OPT\\_DHCPDUMP](#) (Seite 271)  
[OPT\\_DIG](#) (Seite 267)  
[OPT\\_FLASHROM](#) (Seite 273)  
[OPT\\_I2CTOOLS](#) (Seite 273)  
[OPT\\_IWLWEEPROM](#) (Seite 273)  
[OPT\\_LNSTAT](#) (Seite 268)  
[OPT\\_NETIO](#) (Seite 268)  
[OPT\\_NGREP](#) (Seite 268)  
[OPT\\_NMAP](#) (Seite 268)  
[OPT\\_OPENSSL](#) (Seite 274)  
[OPT\\_REAVER](#) (Seite 274)  
[OPT\\_SOCAT](#) (Seite 270)  
[OPT\\_TRACEPATH](#) (Seite 270)

OPT\_ARP  
OPT\_BCRELAY  
OPT\_ETHTOOL  
OPT\_NETSTAT  
OPT\_SERIAL  
OPT\_TRACEROUTE  
OPT\_TRACEROUTE6  
WGET\_SSL

## Package UMTS

### Neue Variablen

### Gelöschte Variablen

[CIRC\\_x\\_UMTS\\_APN](#) (Seite 277)  
[CIRC\\_x\\_UMTS\\_DIALOUT](#) (Seite 276)

UMTS\_APN  
UMTS\_CHARGEINT  
UMTS\_DIALOUT  
UMTS\_FILTER

UMTS\_HUP\_TIMEOUT  
UMTS\_NAME  
UMTS\_PASSWD  
UMTS\_TIMES  
UMTS\_USEPEERDNS  
UMTS\_USER

## Package USB

### Neue Variablen

### Gelöschte Variablen

USB\_LOWLEVEL

## B.14. Unterschiede Version 4.0.0 und 3.10.7

## Package ADVANCED\_NETWORKING

### Neue Variablen

### Gelöschte Variablen

DSA\_N (Seite ??)  
DSA\_x\_BRIDGE (Seite ??)  
DSA\_x\_DEV (Seite ??)  
DSA\_x\_GROUP\_N (Seite ??)  
DSA\_x\_GROUP\_x\_PORT\_N (Seite ??)  
DSA\_x\_GROUP\_x\_PORT\_x\_DEV (Seite ??)  
OPT\_DSA (Seite ??)

## Package BASE

### Neue Variablen

### Gelöschte Variablen

LUATESTS\_RUNATBOOTTIME (Seite ??)  
LUA\_VERSION (Seite ??)  
NET\_PREFIX\_ULA\_SAVEDIR (Seite ??)  
[NET\\_PREFIX\\_x\\_NAME](#) (Seite 47)  
[NET\\_PREFIX\\_x\\_STATIC\\_IPV4](#) (Seite 47)  
[NET\\_PREFIX\\_x\\_STATIC\\_IPV6](#) (Seite 47)  
[NET\\_PREFIX\\_x\\_TYPE](#) (Seite 47)  
[NET\\_PREFIX\\_x\\_ULA\\_DEV](#) (Seite 48)  
OPT\_LUA (Seite ??)  
OPT\_LUATESTS (Seite ??)  
[OPT\\_NET\\_PREFIX](#) (Seite 46)  
OPT\_NET\_PREFIX\_ULA (Seite ??)  
[RTC\\_SYNC](#) (Seite 31)

UCLIBC\_COMPAT

## Package CIRCUITS

### Neue Variablen

### Gelöschte Variablen

CIRC\_x\_NET\_IPV4\_ADDRESS (Seite ??)  
CIRC\_x\_NET\_IPV6\_ADDRESS (Seite ??)

CIRC\_x\_NET\_ADDRESS\_IPV4  
CIRC\_x\_NET\_ADDRESS\_IPV6

## B. Anhänge der optionalen Pakete

CIRC\_x\_NET\_IPV6\_ADVERTISE\_PREFIX (Seite ??)  
CIRC\_x\_NET\_IPV6\_ADVERTISE\_PREFIX\_ON\_LINK  
(Seite ??)  
CIRC\_x\_NET\_IPV6\_ADVERTISE\_PREFIX\_  
PREFERRED\_LIFETIME (Seite ??)  
CIRC\_x\_NET\_IPV6\_ADVERTISE\_PREFIX\_VALID\_  
LIFETIME (Seite ??)

### Package CERT

#### Neue Variablen

CERT\_X509\_MOZILLA (Seite 128)  
OPT\_CERT (Seite 128)  
OPT\_CERT\_X509 (Seite 128)

#### Gelöschte Variablen

### Package CHRONY

#### Neue Variablen

#### Gelöschte Variablen

CHRONY\_BIOS\_TIME

### Package DNS\_DHCP

#### Neue Variablen

#### Gelöschte Variablen

CIRC\_x\_NET\_IPV6\_ADVERTISE\_DNS (Seite ??)  
DHCP\_DNS\_SERVERS (Seite 139)  
DHCP\_EXTRA\_RANGE\_x\_DNS\_SERVERS (Seite 141)  
DHCP\_EXTRA\_RANGE\_x\_NTP\_SERVERS (Seite 141)  
DHCP\_EXTRA\_RANGE\_x\_WINS\_SERVERS (Seite 141)  
DHCP\_NTP\_SERVERS (Seite 139)  
DHCP\_RANGE\_x\_DNS\_SERVERS (Seite 140)  
DHCP\_RANGE\_x\_NTP\_SERVERS (Seite 140)  
DHCP\_RANGE\_x\_WINS\_SERVERS (Seite 140)  
DHCP\_WINS\_SERVERS (Seite 139)

DHCP\_EXTRA\_RANGE\_x\_DNS\_SERVER  
DHCP\_EXTRA\_RANGE\_x\_NTP\_SERVER  
DHCP\_RANGE\_x\_DNS\_SERVER1  
DHCP\_RANGE\_x\_DNS\_SERVER2  
DHCP\_RANGE\_x\_NTP\_SERVER  
DHCP\_WINSERVER1  
DHCP\_WINSERVER2

### Package IPV6

#### Neue Variablen

#### Gelöschte Variablen

CIRC\_x\_TUN6IN4\_SIXXS\_LOCALV6  
CIRC\_x\_TUN6IN4\_SIXXS\_PASSWORD  
CIRC\_x\_TUN6IN4\_SIXXS\_PREFIX  
CIRC\_x\_TUN6IN4\_SIXXS\_REMOTEV6  
CIRC\_x\_TUN6IN4\_SIXXS\_TIMEOUT  
CIRC\_x\_TUN6IN4\_SIXXS\_TUNNELID  
CIRC\_x\_TUN6IN4\_SIXXS\_USERID

### Package ISDN

### Neue Variablen

[ISDN\\_x\\_IO](#) (Seite 180)  
[ISDN\\_x\\_IO0](#) (Seite 180)  
[ISDN\\_x\\_IO1](#) (Seite 180)  
[ISDN\\_x\\_IP](#) (Seite 182)  
[ISDN\\_x\\_IRQ](#) (Seite ??)  
[ISDN\\_x\\_MEM](#) (Seite 180)  
[ISDN\\_x\\_PORT](#) (Seite 182)  
[ISDN\\_x\\_TYPE](#) (Seite 180)

### Gelöschte Variablen

ISDN\_IO  
ISDN\_IO0  
ISDN\_IO1  
ISDN\_IP  
ISDN\_IRQ  
ISDN\_MEM  
ISDN\_PORT  
ISDN\_TYPE

## Package OPENVPN

### Neue Variablen

[OPENVPN\\_x\\_CHECK\\_REPLAY](#) (Seite 216)

### Gelöschte Variablen

## Package PROXY

### Neue Variablen

[IMPROXY\\_DOWNSTREAM\\_DEV](#) (Seite ??)  
[IMPROXY\\_ENABLE\\_IGMPV3](#) (Seite ??)  
[IMPROXY\\_ENABLE\\_MLD](#) (Seite ??)  
[IMPROXY\\_UPSTREAM\\_DEV](#) (Seite ??)  
[OPT\\_IMPROXY](#) (Seite ??)  
[SIPROXD\\_N](#) (Seite ??)  
[SIPROXD\\_x\\_ALLOW\\_REG\\_N](#) (Seite ??)  
[SIPROXD\\_x\\_ALLOW\\_REG\\_x](#) (Seite ??)  
[SIPROXD\\_x\\_DEV\\_IN](#) (Seite ??)  
[SIPROXD\\_x\\_DEV\\_OUT](#) (Seite ??)  
[SIPROXD\\_x\\_RTP\\_PORT\\_MAX](#) (Seite ??)  
[SIPROXD\\_x\\_RTP\\_PORT\\_MIN](#) (Seite ??)  
[SIPROXD\\_x\\_SIP\\_PORT](#) (Seite ??)  
[SIPROXD\\_x\\_TRANSPARENT](#) (Seite ??)  
[SIPROXD\\_x\\_USER\\_N](#) (Seite ??)  
[SIPROXD\\_x\\_USER\\_x\\_NAME](#) (Seite ??)  
[SIPROXD\\_x\\_USER\\_x\\_PASS](#) (Seite ??)

### Gelöschte Variablen

## Package TOOLS

### Neue Variablen

[OPT\\_BMON](#) (Seite 266)  
[OPT\\_FLASHROM](#) (Seite 273)  
[OPT\\_NMAP](#) (Seite 268)

### Gelöschte Variablen

## B.15. Unterschiede Version 4.0.0 und 3.10.8

## Package ADVANCED\_NETWORKING

### Neue Variablen

DSA\_N (Seite ??)  
DSA\_x\_BRIDGE (Seite ??)  
DSA\_x\_DEV (Seite ??)  
DSA\_x\_GROUP\_N (Seite ??)  
DSA\_x\_GROUP\_x\_PORT\_N (Seite ??)  
DSA\_x\_GROUP\_x\_PORT\_x\_DEV (Seite ??)  
OPT\_DSA (Seite ??)

### Gelöschte Variablen

## Package BASE

### Neue Variablen

LUATESTS\_RUNATBOOTTIME (Seite ??)  
LUA\_VERSION (Seite ??)  
NET\_PREFIX\_ULA\_SAVEDIR (Seite ??)  
[NET\\_PREFIX\\_x\\_NAME](#) (Seite 47)  
[NET\\_PREFIX\\_x\\_STATIC\\_IPV4](#) (Seite 47)  
[NET\\_PREFIX\\_x\\_STATIC\\_IPV6](#) (Seite 47)  
[NET\\_PREFIX\\_x\\_TYPE](#) (Seite 47)  
[NET\\_PREFIX\\_x\\_ULA\\_DEV](#) (Seite 48)  
OPT\_LUA (Seite ??)  
OPT\_LUATESTS (Seite ??)  
[OPT\\_NET\\_PREFIX](#) (Seite 46)  
OPT\_NET\_PREFIX\_ULA (Seite ??)  
[RTC\\_SYNC](#) (Seite 31)

### Gelöschte Variablen

## Package CIRCUITS

### Neue Variablen

CIRC\_x\_NET\_IPV4\_ADDRESS (Seite ??)  
CIRC\_x\_NET\_IPV6\_ADDRESS (Seite ??)  
CIRC\_x\_NET\_IPV6\_ADVERTISE\_PREFIX (Seite ??)  
CIRC\_x\_NET\_IPV6\_ADVERTISE\_PREFIX\_ON\_LINK  
(Seite ??)  
CIRC\_x\_NET\_IPV6\_ADVERTISE\_PREFIX\_  
PREFERRED\_LIFETIME (Seite ??)  
CIRC\_x\_NET\_IPV6\_ADVERTISE\_PREFIX\_VALID\_  
LIFETIME (Seite ??)

### Gelöschte Variablen

CIRC\_x\_NET\_ADDRESS\_IPV4  
CIRC\_x\_NET\_ADDRESS\_IPV6

## Package CHRONY

### Neue Variablen

### Gelöschte Variablen

CHRONY\_BIOS\_TIME

## Package DNS\_DHCP

### Neue Variablen

CIRC\_x\_NET\_IPV6\_ADVERTISE\_DNS (Seite ??)  
DHCP\_DNS\_SERVERS (Seite 139)  
DHCP\_EXTRA\_RANGE\_x\_DNS\_SERVERS (Seite 141)  
DHCP\_EXTRA\_RANGE\_x\_NTP\_SERVERS (Seite 141)  
DHCP\_EXTRA\_RANGE\_x\_WINS\_SERVERS (Seite 141)  
DHCP\_NTP\_SERVERS (Seite 139)  
DHCP\_RANGE\_x\_DNS\_SERVERS (Seite 140)  
DHCP\_RANGE\_x\_NTP\_SERVERS (Seite 140)  
DHCP\_RANGE\_x\_WINS\_SERVERS (Seite 140)  
DHCP\_WINS\_SERVERS (Seite 139)

### Gelöschte Variablen

DHCP\_EXTRA\_RANGE\_x\_DNS\_SERVER  
DHCP\_EXTRA\_RANGE\_x\_NTP\_SERVER  
DHCP\_RANGE\_x\_DNS\_SERVER1  
DHCP\_RANGE\_x\_DNS\_SERVER2  
DHCP\_RANGE\_x\_NTP\_SERVER  
DHCP\_WINS\_SERVER1  
DHCP\_WINS\_SERVER2

## Package IPV6

### Neue Variablen

### Gelöschte Variablen

CIRC\_x\_TUN6IN4\_SIXXS\_LOCALV6  
CIRC\_x\_TUN6IN4\_SIXXS\_PASSWORD  
CIRC\_x\_TUN6IN4\_SIXXS\_PREFIX  
CIRC\_x\_TUN6IN4\_SIXXS\_REMOTEV6  
CIRC\_x\_TUN6IN4\_SIXXS\_TIMEOUT  
CIRC\_x\_TUN6IN4\_SIXXS\_TUNNELID  
CIRC\_x\_TUN6IN4\_SIXXS\_USERID

## Package ISDN

### Neue Variablen

### Gelöschte Variablen

ISDN\_x\_IO (Seite 180)  
ISDN\_x\_IO0 (Seite 180)  
ISDN\_x\_IO1 (Seite 180)  
ISDN\_x\_IP (Seite 182)  
ISDN\_x\_IRQ (Seite ??)  
ISDN\_x\_MEM (Seite 180)  
ISDN\_x\_PORT (Seite 182)  
ISDN\_x\_TYPE (Seite 180)

ISDN\_IO  
ISDN\_IO0  
ISDN\_IO1  
ISDN\_IP  
ISDN\_IRQ  
ISDN\_MEM  
ISDN\_PORT  
ISDN\_TYPE

## Package PROXY

### Neue Variablen

### Gelöschte Variablen

IMPROXY\_DOWNSTREAM\_DEV (Seite ??)  
IMPROXY\_ENABLE\_IGMPV3 (Seite ??)  
IMPROXY\_ENABLE\_MLD (Seite ??)  
IMPROXY\_UPSTREAM\_DEV (Seite ??)  
OPT\_IMPROXY (Seite ??)  
SIPROXD\_N (Seite ??)  
SIPROXD\_x\_ALLOW\_REG\_N (Seite ??)  
SIPROXD\_x\_ALLOW\_REG\_x (Seite ??)  
SIPROXD\_x\_DEV\_IN (Seite ??)  
SIPROXD\_x\_DEV\_OUT (Seite ??)  
SIPROXD\_x\_RTP\_PORT\_MAX (Seite ??)  
SIPROXD\_x\_RTP\_PORT\_MIN (Seite ??)  
SIPROXD\_x\_SIP\_PORT (Seite ??)



SIPROXD\_x\_TRANSPARENT (Seite ??)  
SIPROXD\_x\_USER\_N (Seite ??)  
SIPROXD\_x\_USER\_x\_NAME (Seite ??)  
SIPROXD\_x\_USER\_x\_PASS (Seite ??)

## Package TOOLS

### Neue Variablen

[OPT\\_BMON](#) (Seite 266)  
[OPT\\_NMAP](#) (Seite 268)

### Gelöschte Variablen

## B.16. Unterschiede Version 4.0.0 und 3.10.9

## Package ADVANCED\_NETWORKING

### Neue Variablen

DSA\_N (Seite ??)  
DSA\_x\_BRIDGE (Seite ??)  
DSA\_x\_DEV (Seite ??)  
DSA\_x\_GROUP\_N (Seite ??)  
DSA\_x\_GROUP\_x\_PORT\_N (Seite ??)  
DSA\_x\_GROUP\_x\_PORT\_x\_DEV (Seite ??)  
OPT\_DSA (Seite ??)

### Gelöschte Variablen

## Package BASE

### Neue Variablen

LUATESTS\_RUNATBOOTTIME (Seite ??)  
LUA\_VERSION (Seite ??)  
NET\_PREFIX\_ULA\_SAVEDIR (Seite ??)  
[NET\\_PREFIX\\_x\\_NAME](#) (Seite 47)  
[NET\\_PREFIX\\_x\\_STATIC\\_IPV4](#) (Seite 47)  
[NET\\_PREFIX\\_x\\_STATIC\\_IPV6](#) (Seite 47)  
[NET\\_PREFIX\\_x\\_TYPE](#) (Seite 47)  
[NET\\_PREFIX\\_x\\_ULA\\_DEV](#) (Seite 48)  
OPT\_LUA (Seite ??)  
OPT\_LUATESTS (Seite ??)  
[OPT\\_NET\\_PREFIX](#) (Seite 46)  
OPT\_NET\_PREFIX\_ULA (Seite ??)  
[RTC\\_SYNC](#) (Seite 31)

### Gelöschte Variablen

## Package CIRCUITS

### Neue Variablen

CIRC\_x\_NET\_IPV4\_ADDRESS (Seite ??)  
CIRC\_x\_NET\_IPV6\_ADDRESS (Seite ??)  
CIRC\_x\_NET\_IPV6\_ADVERTISE\_PREFIX (Seite ??)

### Gelöschte Variablen

CIRC\_x\_NET\_ADDRESS\_IPV4  
CIRC\_x\_NET\_ADDRESS\_IPV6

CIRC\_x\_NET\_IPV6\_ADVERTISE\_PREFIX\_ON\_LINK  
(Seite ??)  
CIRC\_x\_NET\_IPV6\_ADVERTISE\_PREFIX\_  
PREFERRED\_LIFETIME (Seite ??)  
CIRC\_x\_NET\_IPV6\_ADVERTISE\_PREFIX\_VALID\_  
LIFETIME (Seite ??)

## Package CHRONY

### Neue Variablen

### Gelöschte Variablen

CHRONY\_BIOS\_TIME

## Package DNS\_DHCP

### Neue Variablen

### Gelöschte Variablen

CIRC\_x\_NET\_IPV6\_ADVERTISE\_DNS (Seite ??)  
[DHCP\\_DNS\\_SERVERS](#) (Seite 139)  
[DHCP\\_EXTRA\\_RANGE\\_x\\_DNS\\_SERVERS](#) (Seite 141)  
[DHCP\\_EXTRA\\_RANGE\\_x\\_NTP\\_SERVERS](#) (Seite 141)  
[DHCP\\_EXTRA\\_RANGE\\_x\\_WINS\\_SERVERS](#) (Seite 141)  
[DHCP\\_NTP\\_SERVERS](#) (Seite 139)  
[DHCP\\_RANGE\\_x\\_DNS\\_SERVERS](#) (Seite 140)  
[DHCP\\_RANGE\\_x\\_NTP\\_SERVERS](#) (Seite 140)  
[DHCP\\_RANGE\\_x\\_WINS\\_SERVERS](#) (Seite 140)  
[DHCP\\_WINS\\_SERVERS](#) (Seite 139)

DHCP\_EXTRA\_RANGE\_x\_DNS\_SERVER  
DHCP\_EXTRA\_RANGE\_x\_NTP\_SERVER  
DHCP\_RANGE\_x\_DNS\_SERVER1  
DHCP\_RANGE\_x\_DNS\_SERVER2  
DHCP\_RANGE\_x\_NTP\_SERVER  
DHCP\_WINS\_SERVER1  
DHCP\_WINS\_SERVER2

## Package IPV6

### Neue Variablen

### Gelöschte Variablen

CIRC\_x\_TUN6IN4\_SIXXS\_LOCALV6  
CIRC\_x\_TUN6IN4\_SIXXS\_PASSWORD  
CIRC\_x\_TUN6IN4\_SIXXS\_PREFIX  
CIRC\_x\_TUN6IN4\_SIXXS\_REMOTEV6  
CIRC\_x\_TUN6IN4\_SIXXS\_TIMEOUT  
CIRC\_x\_TUN6IN4\_SIXXS\_TUNNELID  
CIRC\_x\_TUN6IN4\_SIXXS\_USERID

## Package ISDN

### Neue Variablen

### Gelöschte Variablen

[ISDN\\_x\\_IO](#) (Seite 180)  
[ISDN\\_x\\_IO0](#) (Seite 180)  
[ISDN\\_x\\_IO1](#) (Seite 180)  
[ISDN\\_x\\_IP](#) (Seite 182)  
[ISDN\\_x\\_IRQ](#) (Seite ??)  
[ISDN\\_x\\_MEM](#) (Seite 180)  
[ISDN\\_x\\_PORT](#) (Seite 182)  
[ISDN\\_x\\_TYPE](#) (Seite 180)

ISDN\_IO  
ISDN\_IO0  
ISDN\_IO1  
ISDN\_IP  
ISDN\_IRQ  
ISDN\_MEM  
ISDN\_PORT  
ISDN\_TYPE

## Package PROXY

### Neue Variablen

IMPROXY\_DOWNSTREAM\_DEV (Seite ??)  
IMPROXY\_ENABLE\_IGMPV3 (Seite ??)  
IMPROXY\_ENABLE\_MLD (Seite ??)  
IMPROXY\_UPSTREAM\_DEV (Seite ??)  
OPT\_IMPROXY (Seite ??)  
SIPROXD\_N (Seite ??)  
SIPROXD\_x\_ALLOW\_REG\_N (Seite ??)  
SIPROXD\_x\_ALLOW\_REG\_x (Seite ??)  
SIPROXD\_x\_DEV\_IN (Seite ??)  
SIPROXD\_x\_DEV\_OUT (Seite ??)  
SIPROXD\_x\_RTP\_PORT\_MAX (Seite ??)  
SIPROXD\_x\_RTP\_PORT\_MIN (Seite ??)  
SIPROXD\_x\_SIP\_PORT (Seite ??)  
SIPROXD\_x\_TRANSPARENT (Seite ??)  
SIPROXD\_x\_USER\_N (Seite ??)  
SIPROXD\_x\_USER\_x\_NAME (Seite ??)  
SIPROXD\_x\_USER\_x\_PASS (Seite ??)

### Gelöschte Variablen

## Package TOOLS

### Neue Variablen

[OPT\\_BMON](#) (Seite 266)

### Gelöschte Variablen

## B.17. Unterschiede Version 4.0.0 und 3.10.10

## Package ADVANCED\_NETWORKING

### Neue Variablen

DSA\_N (Seite ??)  
DSA\_x\_BRIDGE (Seite ??)  
DSA\_x\_DEV (Seite ??)  
DSA\_x\_GROUP\_N (Seite ??)  
DSA\_x\_GROUP\_x\_PORT\_N (Seite ??)  
DSA\_x\_GROUP\_x\_PORT\_x\_DEV (Seite ??)  
OPT\_DSA (Seite ??)

### Gelöschte Variablen

## Package BASE

### Neue Variablen

LUATESTS\_RUNATBOOTTIME (Seite ??)  
LUA\_VERSION (Seite ??)  
NET\_PREFIX\_ULA\_SAVEDIR (Seite ??)  
[NET\\_PREFIX\\_x\\_NAME](#) (Seite 47)

### Gelöschte Variablen

[NET\\_PREFIX\\_x\\_STATIC\\_IPV4](#) (Seite 47)  
[NET\\_PREFIX\\_x\\_STATIC\\_IPV6](#) (Seite 47)  
[NET\\_PREFIX\\_x\\_TYPE](#) (Seite 47)  
[NET\\_PREFIX\\_x\\_ULA\\_DEV](#) (Seite 48)  
[OPT\\_LUA](#) (Seite ??)  
[OPT\\_LUATESTS](#) (Seite ??)  
[OPT\\_NET\\_PREFIX](#) (Seite 46)  
[OPT\\_NET\\_PREFIX\\_ULA](#) (Seite ??)  
[RTC\\_SYNC](#) (Seite 31)

## Package CIRCUITS

### Neue Variablen

[CIRC\\_x\\_NET\\_IPV4\\_ADDRESS](#) (Seite ??)  
[CIRC\\_x\\_NET\\_IPV6\\_ADDRESS](#) (Seite ??)  
[CIRC\\_x\\_NET\\_IPV6\\_ADVERTISE\\_PREFIX](#) (Seite ??)  
[CIRC\\_x\\_NET\\_IPV6\\_ADVERTISE\\_PREFIX\\_ON\\_LINK](#)  
(Seite ??)  
[CIRC\\_x\\_NET\\_IPV6\\_ADVERTISE\\_PREFIX\\_-  
PREFERRED\\_LIFETIME](#) (Seite ??)  
[CIRC\\_x\\_NET\\_IPV6\\_ADVERTISE\\_PREFIX\\_VALID\\_-  
LIFETIME](#) (Seite ??)

### Gelöschte Variablen

[CIRC\\_x\\_NET\\_ADDRESS\\_IPV4](#)  
[CIRC\\_x\\_NET\\_ADDRESS\\_IPV6](#)

## Package CHRONY

### Neue Variablen

### Gelöschte Variablen

[CHRONY\\_BIOS\\_TIME](#)

## Package DNS\_DHCP

### Neue Variablen

[CIRC\\_x\\_NET\\_IPV6\\_ADVERTISE\\_DNS](#) (Seite ??)  
[DHCP\\_DNS\\_SERVERS](#) (Seite 139)  
[DHCP\\_EXTRA\\_RANGE\\_x\\_DNS\\_SERVERS](#) (Seite 141)  
[DHCP\\_EXTRA\\_RANGE\\_x\\_NTP\\_SERVERS](#) (Seite 141)  
[DHCP\\_EXTRA\\_RANGE\\_x\\_WINS\\_SERVERS](#) (Seite 141)  
[DHCP\\_NTP\\_SERVERS](#) (Seite 139)  
[DHCP\\_RANGE\\_x\\_DNS\\_SERVERS](#) (Seite 140)  
[DHCP\\_RANGE\\_x\\_NTP\\_SERVERS](#) (Seite 140)  
[DHCP\\_RANGE\\_x\\_WINS\\_SERVERS](#) (Seite 140)  
[DHCP\\_WINS\\_SERVERS](#) (Seite 139)

### Gelöschte Variablen

[DHCP\\_EXTRA\\_RANGE\\_x\\_DNS\\_SERVER](#)  
[DHCP\\_EXTRA\\_RANGE\\_x\\_NTP\\_SERVER](#)  
[DHCP\\_RANGE\\_x\\_DNS\\_SERVER1](#)  
[DHCP\\_RANGE\\_x\\_DNS\\_SERVER2](#)  
[DHCP\\_RANGE\\_x\\_NTP\\_SERVER](#)  
[DHCP\\_WINSERVER1](#)  
[DHCP\\_WINSERVER2](#)

## Package IPV6

### Neue Variablen

### Gelöschte Variablen

[CIRC\\_x\\_TUN6IN4\\_SIXXS\\_LOCALV6](#)  
[CIRC\\_x\\_TUN6IN4\\_SIXXS\\_PASSWORD](#)  
[CIRC\\_x\\_TUN6IN4\\_SIXXS\\_PREFIX](#)  
[CIRC\\_x\\_TUN6IN4\\_SIXXS\\_REMOTEV6](#)  
[CIRC\\_x\\_TUN6IN4\\_SIXXS\\_TIMEOUT](#)

CIRC\_x\_TUN6IN4\_SIXXS\_TUNNELID  
CIRC\_x\_TUN6IN4\_SIXXS\_USERID

## Package ISDN

### Neue Variablen

ISDN\_x\_IO (Seite 180)  
ISDN\_x\_IO0 (Seite 180)  
ISDN\_x\_IO1 (Seite 180)  
ISDN\_x\_IP (Seite 182)  
ISDN\_x\_IRQ (Seite ??)  
ISDN\_x\_MEM (Seite 180)  
ISDN\_x\_PORT (Seite 182)  
ISDN\_x\_TYPE (Seite 180)

### Gelöschte Variablen

ISDN\_IO0\_x  
ISDN\_IO1\_x  
ISDN\_IO\_x  
ISDN\_IP  
ISDN\_IRQ\_x  
ISDN\_MEM\_x  
ISDN\_PORT  
ISDN\_TYPE\_x

## Package PROXY

### Neue Variablen

IMPROXY\_DOWNSTREAM\_DEV (Seite ??)  
IMPROXY\_ENABLE\_IGMPV3 (Seite ??)  
IMPROXY\_ENABLE\_MLD (Seite ??)  
IMPROXY\_UPSTREAM\_DEV (Seite ??)  
OPT\_IMPROXY (Seite ??)  
SIPROXD\_N (Seite ??)  
SIPROXD\_x\_ALLOW\_REG\_N (Seite ??)  
SIPROXD\_x\_ALLOW\_REG\_x (Seite ??)  
SIPROXD\_x\_DEV\_IN (Seite ??)  
SIPROXD\_x\_DEV\_OUT (Seite ??)  
SIPROXD\_x\_RTP\_PORT\_MAX (Seite ??)  
SIPROXD\_x\_RTP\_PORT\_MIN (Seite ??)  
SIPROXD\_x\_SIP\_PORT (Seite ??)  
SIPROXD\_x\_TRANSPARENT (Seite ??)  
SIPROXD\_x\_USER\_N (Seite ??)  
SIPROXD\_x\_USER\_x\_NAME (Seite ??)  
SIPROXD\_x\_USER\_x\_PASS (Seite ??)

### Gelöschte Variablen

## Package TOOLS

### Neue Variablen

OPT\_BMON (Seite 266)

### Gelöschte Variablen

## B.18. Unterschiede Version 4.0.0 und 3.10.11

## Package ADVANCED\_NETWORKING

### Neue Variablen

DSA\_N (Seite ??)

### Gelöschte Variablen

DSA\_x\_BRIDGE (Seite ??)  
DSA\_x\_DEV (Seite ??)  
DSA\_x\_GROUP\_N (Seite ??)  
DSA\_x\_GROUP\_x\_PORT\_N (Seite ??)  
DSA\_x\_GROUP\_x\_PORT\_x\_DEV (Seite ??)  
OPT\_DSA (Seite ??)

## Package BASE

### Neue Variablen

LUATESTS\_RUNATBOOTTIME (Seite ??)  
LUA\_VERSION (Seite ??)  
NET\_PREFIX\_ULA\_SAVEDIR (Seite ??)  
[NET\\_PREFIX\\_x\\_NAME](#) (Seite 47)  
[NET\\_PREFIX\\_x\\_STATIC\\_IPV4](#) (Seite 47)  
[NET\\_PREFIX\\_x\\_STATIC\\_IPV6](#) (Seite 47)  
[NET\\_PREFIX\\_x\\_TYPE](#) (Seite 47)  
[NET\\_PREFIX\\_x\\_ULA\\_DEV](#) (Seite 48)  
OPT\_LUA (Seite ??)  
OPT\_LUATESTS (Seite ??)  
[OPT\\_NET\\_PREFIX](#) (Seite 46)  
OPT\_NET\_PREFIX\_ULA (Seite ??)  
[RTC\\_SYNC](#) (Seite 31)

### Gelöschte Variablen

## Package CIRCUITS

### Neue Variablen

CIRC\_x\_NET\_IPV4\_ADDRESS (Seite ??)  
CIRC\_x\_NET\_IPV6\_ADDRESS (Seite ??)  
CIRC\_x\_NET\_IPV6\_ADVERTISE\_PREFIX (Seite ??)  
CIRC\_x\_NET\_IPV6\_ADVERTISE\_PREFIX\_ON\_LINK  
(Seite ??)  
CIRC\_x\_NET\_IPV6\_ADVERTISE\_PREFIX\_  
PREFERRED\_LIFETIME (Seite ??)  
CIRC\_x\_NET\_IPV6\_ADVERTISE\_PREFIX\_VALID\_  
LIFETIME (Seite ??)

### Gelöschte Variablen

CIRC\_x\_NET\_ADDRESS\_IPV4  
CIRC\_x\_NET\_ADDRESS\_IPV6

## Package CHRONY

### Neue Variablen

### Gelöschte Variablen

CHRONY\_BIOS\_TIME

## Package DNS\_DHCP

### Neue Variablen

CIRC\_x\_NET\_IPV6\_ADVERTISE\_DNS (Seite ??)  
[DHCP\\_DNS\\_SERVERS](#) (Seite 139)  
[DHCP\\_EXTRA\\_RANGE\\_x\\_DNS\\_SERVERS](#) (Seite 141)  
[DHCP\\_EXTRA\\_RANGE\\_x\\_NTP\\_SERVERS](#) (Seite 141)  
[DHCP\\_EXTRA\\_RANGE\\_x\\_WINS\\_SERVERS](#) (Seite 141)

### Gelöschte Variablen

DHCP\_EXTRA\_RANGE\_x\_DNS\_SERVER  
DHCP\_EXTRA\_RANGE\_x\_NTP\_SERVER  
DHCP\_RANGE\_x\_DNS\_SERVER1  
DHCP\_RANGE\_x\_DNS\_SERVER2  
DHCP\_RANGE\_x\_NTP\_SERVER

## B. Anhänge der optionalen Pakete

[DHCP\\_NTP\\_SERVERS](#) (Seite 139)  
[DHCP\\_RANGE\\_x\\_DNS\\_SERVERS](#) (Seite 140)  
[DHCP\\_RANGE\\_x\\_NTP\\_SERVERS](#) (Seite 140)  
[DHCP\\_RANGE\\_x\\_WINS\\_SERVERS](#) (Seite 140)  
[DHCP\\_WINS\\_SERVERS](#) (Seite 139)

DHCP\_WINSSERVER1  
DHCP\_WINSSERVER2

### Package PROXY

#### Neue Variablen

IMPROXY\_DOWNSTREAM\_DEV (Seite ??)  
IMPROXY\_ENABLE\_IGMPV3 (Seite ??)  
IMPROXY\_ENABLE\_MLD (Seite ??)  
IMPROXY\_UPSTREAM\_DEV (Seite ??)  
OPT\_IMPROXY (Seite ??)  
SIPROXD\_N (Seite ??)  
SIPROXD\_x\_ALLOW\_REG\_N (Seite ??)  
SIPROXD\_x\_ALLOW\_REG\_x (Seite ??)  
SIPROXD\_x\_DEV\_IN (Seite ??)  
SIPROXD\_x\_DEV\_OUT (Seite ??)  
SIPROXD\_x\_RTP\_PORT\_MAX (Seite ??)  
SIPROXD\_x\_RTP\_PORT\_MIN (Seite ??)  
SIPROXD\_x\_SIP\_PORT (Seite ??)  
SIPROXD\_x\_TRANSPARENT (Seite ??)  
SIPROXD\_x\_USER\_N (Seite ??)  
SIPROXD\_x\_USER\_x\_NAME (Seite ??)  
SIPROXD\_x\_USER\_x\_PASS (Seite ??)

#### Gelöschte Variablen

### Package TOOLS

#### Neue Variablen

[OPT\\_BMON](#) (Seite 266)

#### Gelöschte Variablen

## B.19. Unterschiede Version 4.0.0 und 3.10.12

### Package ADVANCED\_NETWORKING

#### Neue Variablen

DSA\_N (Seite ??)  
DSA\_x\_BRIDGE (Seite ??)  
DSA\_x\_DEV (Seite ??)  
DSA\_x\_GROUP\_N (Seite ??)  
DSA\_x\_GROUP\_x\_PORT\_N (Seite ??)  
DSA\_x\_GROUP\_x\_PORT\_x\_DEV (Seite ??)  
OPT\_DSA (Seite ??)

#### Gelöschte Variablen

### Package BASE

#### Neue Variablen

#### Gelöschte Variablen

LUATESTS\_RUNATBOOTTIME (Seite ??)  
LUA\_VERSION (Seite ??)  
OPT\_LUA (Seite ??)  
OPT\_LUATESTS (Seite ??)  
[RTC\\_SYNC](#) (Seite 31)

## Package CIRCUITS

### Neue Variablen

CIRC\_x\_NET\_IPV4\_ADDRESS (Seite ??)  
CIRC\_x\_NET\_IPV6\_ADDRESS (Seite ??)  
CIRC\_x\_NET\_IPV6\_ADVERTISE\_PREFIX (Seite ??)  
CIRC\_x\_NET\_IPV6\_ADVERTISE\_PREFIX\_ON\_LINK  
(Seite ??)  
CIRC\_x\_NET\_IPV6\_ADVERTISE\_PREFIX\_  
PREFERRED\_LIFETIME (Seite ??)  
CIRC\_x\_NET\_IPV6\_ADVERTISE\_PREFIX\_VALID\_  
LIFETIME (Seite ??)

### Gelöschte Variablen

CIRC\_x\_NET\_ADDRESS\_IPV4  
CIRC\_x\_NET\_ADDRESS\_IPV6

## Package CHRONY

### Neue Variablen

### Gelöschte Variablen

CHRONY\_BIOS\_TIME

## Package DNS\_DHCP

### Neue Variablen

CIRC\_x\_NET\_IPV6\_ADVERTISE\_DNS (Seite ??)  
[DHCP\\_DNS\\_SERVERS](#) (Seite 139)  
[DHCP\\_EXTRA\\_RANGE\\_x\\_DNS\\_SERVERS](#) (Seite 141)  
[DHCP\\_EXTRA\\_RANGE\\_x\\_NTP\\_SERVERS](#) (Seite 141)  
[DHCP\\_EXTRA\\_RANGE\\_x\\_WINS\\_SERVERS](#) (Seite 141)  
[DHCP\\_NTP\\_SERVERS](#) (Seite 139)  
[DHCP\\_RANGE\\_x\\_DNS\\_SERVERS](#) (Seite 140)  
[DHCP\\_RANGE\\_x\\_NTP\\_SERVERS](#) (Seite 140)  
[DHCP\\_RANGE\\_x\\_WINS\\_SERVERS](#) (Seite 140)  
[DHCP\\_WINS\\_SERVERS](#) (Seite 139)

### Gelöschte Variablen

DHCP\_EXTRA\_RANGE\_x\_DNS\_SERVER  
DHCP\_EXTRA\_RANGE\_x\_NTP\_SERVER  
DHCP\_RANGE\_x\_DNS\_SERVER1  
DHCP\_RANGE\_x\_DNS\_SERVER2  
DHCP\_RANGE\_x\_NTP\_SERVER  
DHCP\_WINSERVER1  
DHCP\_WINSERVER2

## Package PROXY

### Neue Variablen

IMPROXY\_DOWNSTREAM\_DEV (Seite ??)  
IMPROXY\_ENABLE\_IGMPV3 (Seite ??)  
IMPROXY\_ENABLE\_MLD (Seite ??)  
IMPROXY\_UPSTREAM\_DEV (Seite ??)  
OPT\_IMPROXY (Seite ??)  
SIPROXD\_N (Seite ??)  
SIPROXD\_x\_ALLOW\_REG\_N (Seite ??)  
SIPROXD\_x\_ALLOW\_REG\_x (Seite ??)  
SIPROXD\_x\_DEV\_IN (Seite ??)

### Gelöschte Variablen



SIPROXD\_x\_DEV\_OUT (Seite ??)  
SIPROXD\_x\_RTP\_PORT\_MAX (Seite ??)  
SIPROXD\_x\_RTP\_PORT\_MIN (Seite ??)  
SIPROXD\_x\_SIP\_PORT (Seite ??)  
SIPROXD\_x\_TRANSPARENT (Seite ??)  
SIPROXD\_x\_USER\_N (Seite ??)  
SIPROXD\_x\_USER\_x\_NAME (Seite ??)  
SIPROXD\_x\_USER\_x\_PASS (Seite ??)

## Package TOOLS

### Neue Variablen

### Gelöschte Variablen

[OPT\\_BMON](#) (Seite 266)

## B.20. Unterschiede Version 4.0.0 und 3.10.13

## Package ADVANCED\_NETWORKING

### Neue Variablen

### Gelöschte Variablen

DSA\_N (Seite ??)  
DSA\_x\_BRIDGE (Seite ??)  
DSA\_x\_DEV (Seite ??)  
DSA\_x\_GROUP\_N (Seite ??)  
DSA\_x\_GROUP\_x\_PORT\_N (Seite ??)  
DSA\_x\_GROUP\_x\_PORT\_x\_DEV (Seite ??)  
OPT\_DSA (Seite ??)

## Package BASE

### Neue Variablen

### Gelöschte Variablen

OPT\_LUA (Seite ??)

## Package CIRCUITS

### Neue Variablen

### Gelöschte Variablen

CIRC\_x\_NET\_IPV4\_ADDRESS (Seite ??)  
CIRC\_x\_NET\_IPV6\_ADDRESS (Seite ??)  
CIRC\_x\_NET\_IPV6\_ADVERTISE\_PREFIX (Seite ??)  
CIRC\_x\_NET\_IPV6\_ADVERTISE\_PREFIX\_ON\_LINK  
(Seite ??)  
CIRC\_x\_NET\_IPV6\_ADVERTISE\_PREFIX\_  
PREFERRED\_LIFETIME (Seite ??)  
CIRC\_x\_NET\_IPV6\_ADVERTISE\_PREFIX\_VALID\_  
LIFETIME (Seite ??)

CIRC\_x\_NET\_ADDRESS\_IPV4  
CIRC\_x\_NET\_ADDRESS\_IPV6

## Package DNS\_DHCP

### Neue Variablen

CIRC\_x\_NET\_IPV6\_ADVERTISE\_DNS (Seite ??)  
DHCP\_DNS\_SERVERS (Seite 139)  
DHCP\_EXTRA\_RANGE\_x\_DNS\_SERVERS (Seite 141)  
DHCP\_EXTRA\_RANGE\_x\_NTP\_SERVERS (Seite 141)  
DHCP\_EXTRA\_RANGE\_x\_WINS\_SERVERS (Seite 141)  
DHCP\_NTP\_SERVERS (Seite 139)  
DHCP\_RANGE\_x\_DNS\_SERVERS (Seite 140)  
DHCP\_RANGE\_x\_NTP\_SERVERS (Seite 140)  
DHCP\_RANGE\_x\_WINS\_SERVERS (Seite 140)  
DHCP\_WINS\_SERVERS (Seite 139)

### Gelöschte Variablen

DHCP\_EXTRA\_RANGE\_x\_DNS\_SERVER  
DHCP\_EXTRA\_RANGE\_x\_NTP\_SERVER  
DHCP\_RANGE\_x\_DNS\_SERVER1  
DHCP\_RANGE\_x\_DNS\_SERVER2  
DHCP\_RANGE\_x\_NTP\_SERVER  
DHCP\_WINS\_SERVER1  
DHCP\_WINS\_SERVER2

## Package PROXY

### Neue Variablen

IMPROXY\_DOWNSTREAM\_DEV (Seite ??)  
IMPROXY\_ENABLE\_IGMPV3 (Seite ??)  
IMPROXY\_ENABLE\_MLD (Seite ??)  
IMPROXY\_UPSTREAM\_DEV (Seite ??)  
OPT\_IMPROXY (Seite ??)  
SIPROXD\_N (Seite ??)  
SIPROXD\_x\_ALLOW\_REG\_N (Seite ??)  
SIPROXD\_x\_ALLOW\_REG\_x (Seite ??)  
SIPROXD\_x\_DEV\_IN (Seite ??)  
SIPROXD\_x\_DEV\_OUT (Seite ??)  
SIPROXD\_x\_RTP\_PORT\_MAX (Seite ??)  
SIPROXD\_x\_RTP\_PORT\_MIN (Seite ??)  
SIPROXD\_x\_SIP\_PORT (Seite ??)  
SIPROXD\_x\_TRANSPARENT (Seite ??)  
SIPROXD\_x\_USER\_N (Seite ??)  
SIPROXD\_x\_USER\_x\_NAME (Seite ??)  
SIPROXD\_x\_USER\_x\_PASS (Seite ??)

### Gelöschte Variablen

## Package TOOLS

### Neue Variablen

OPT\_BMON (Seite 266)

### Gelöschte Variablen

## B.21. Unterschiede Version 4.0.0 und 3.10.14

## Package ADVANCED\_NETWORKING

### Neue Variablen

DSA\_N (Seite ??)  
DSA\_x\_BRIDGE (Seite ??)  
DSA\_x\_DEV (Seite ??)  
DSA\_x\_GROUP\_N (Seite ??)  
DSA\_x\_GROUP\_x\_PORT\_N (Seite ??)

### Gelöschte Variablen

DSA\_x\_GROUP\_x\_PORT\_x\_DEV (Seite ??)  
OPT\_DSA (Seite ??)

## Package BASE

### Neue Variablen

OPT\_LUA (Seite ??)

### Gelöschte Variablen

## Package CIRCUITS

### Neue Variablen

CIRC\_x\_NET\_IPV4\_ADDRESS (Seite ??)  
CIRC\_x\_NET\_IPV6\_ADDRESS (Seite ??)  
CIRC\_x\_NET\_IPV6\_ADVERTISE\_PREFIX (Seite ??)  
CIRC\_x\_NET\_IPV6\_ADVERTISE\_PREFIX\_ON\_LINK  
(Seite ??)  
CIRC\_x\_NET\_IPV6\_ADVERTISE\_PREFIX\_  
PREFERRED\_LIFETIME (Seite ??)  
CIRC\_x\_NET\_IPV6\_ADVERTISE\_PREFIX\_VALID\_  
LIFETIME (Seite ??)

### Gelöschte Variablen

CIRC\_x\_NET\_ADDRESS\_IPV4  
CIRC\_x\_NET\_ADDRESS\_IPV6

## Package DNS\_DHCP

### Neue Variablen

CIRC\_x\_NET\_IPV6\_ADVERTISE\_DNS (Seite ??)  
[DHCP\\_DNS\\_SERVERS](#) (Seite 139)  
[DHCP\\_EXTRA\\_RANGE\\_x\\_DNS\\_SERVERS](#) (Seite 141)  
[DHCP\\_EXTRA\\_RANGE\\_x\\_NTP\\_SERVERS](#) (Seite 141)  
[DHCP\\_EXTRA\\_RANGE\\_x\\_WINS\\_SERVERS](#) (Seite 141)  
[DHCP\\_NTP\\_SERVERS](#) (Seite 139)  
[DHCP\\_RANGE\\_x\\_DNS\\_SERVERS](#) (Seite 140)  
[DHCP\\_RANGE\\_x\\_NTP\\_SERVERS](#) (Seite 140)  
[DHCP\\_RANGE\\_x\\_WINS\\_SERVERS](#) (Seite 140)  
[DHCP\\_WINS\\_SERVERS](#) (Seite 139)

### Gelöschte Variablen

DHCP\_EXTRA\_RANGE\_x\_DNS\_SERVER  
DHCP\_EXTRA\_RANGE\_x\_NTP\_SERVER  
DHCP\_RANGE\_x\_DNS\_SERVER1  
DHCP\_RANGE\_x\_DNS\_SERVER2  
DHCP\_RANGE\_x\_NTP\_SERVER  
DHCP\_WINSERVER1  
DHCP\_WINSERVER2

## Package PROXY

### Neue Variablen

IMPROXY\_DOWNSTREAM\_DEV (Seite ??)  
IMPROXY\_ENABLE\_IGMPV3 (Seite ??)  
IMPROXY\_ENABLE\_MLD (Seite ??)  
IMPROXY\_UPSTREAM\_DEV (Seite ??)  
OPT\_IMPROXY (Seite ??)  
SIPROXD\_N (Seite ??)  
SIPROXD\_x\_ALLOW\_REG\_N (Seite ??)  
SIPROXD\_x\_ALLOW\_REG\_x (Seite ??)  
SIPROXD\_x\_DEV\_IN (Seite ??)  
SIPROXD\_x\_DEV\_OUT (Seite ??)  
SIPROXD\_x\_RTP\_PORT\_MAX (Seite ??)  
SIPROXD\_x\_RTP\_PORT\_MIN (Seite ??)

### Gelöschte Variablen

SIPROXD\_x\_SIP\_PORT (Seite ??)  
SIPROXD\_x\_TRANSPARENT (Seite ??)  
SIPROXD\_x\_USER\_N (Seite ??)  
SIPROXD\_x\_USER\_x\_NAME (Seite ??)  
SIPROXD\_x\_USER\_x\_PASS (Seite ??)

## Package TOOLS

### Neue Variablen

### Gelöschte Variablen

[OPT\\_BMON](#) (Seite 266)

## B.22. Unterschiede Version 4.0.0 und 3.10.15

## Package ADVANCED\_NETWORKING

### Neue Variablen

### Gelöschte Variablen

DSA\_N (Seite ??)  
DSA\_x\_BRIDGE (Seite ??)  
DSA\_x\_DEV (Seite ??)  
DSA\_x\_GROUP\_N (Seite ??)  
DSA\_x\_GROUP\_x\_PORT\_N (Seite ??)  
DSA\_x\_GROUP\_x\_PORT\_x\_DEV (Seite ??)  
OPT\_DSA (Seite ??)

## Package CIRCUITS

### Neue Variablen

### Gelöschte Variablen

CIRC\_x\_NET\_IPV4\_ADDRESS (Seite ??)  
CIRC\_x\_NET\_IPV6\_ADDRESS (Seite ??)  
CIRC\_x\_NET\_IPV6\_ADVERTISE\_PREFIX (Seite ??)  
CIRC\_x\_NET\_IPV6\_ADVERTISE\_PREFIX\_ON\_LINK  
(Seite ??)  
CIRC\_x\_NET\_IPV6\_ADVERTISE\_PREFIX\_  
PREFERRED\_LIFETIME (Seite ??)  
CIRC\_x\_NET\_IPV6\_ADVERTISE\_PREFIX\_VALID\_  
LIFETIME (Seite ??)

CIRC\_x\_NET\_ADDRESS\_IPV4  
CIRC\_x\_NET\_ADDRESS\_IPV6

## Package DNS\_DHCP

### Neue Variablen

### Gelöschte Variablen

CIRC\_x\_NET\_IPV6\_ADVERTISE\_DNS (Seite ??)  
[DHCP\\_DNS\\_SERVERS](#) (Seite 139)  
[DHCP\\_EXTRA\\_RANGE\\_x\\_DNS\\_SERVERS](#) (Seite 141)  
[DHCP\\_EXTRA\\_RANGE\\_x\\_NTP\\_SERVERS](#) (Seite 141)  
[DHCP\\_EXTRA\\_RANGE\\_x\\_WINS\\_SERVERS](#) (Seite 141)  
[DHCP\\_NTP\\_SERVERS](#) (Seite 139)  
[DHCP\\_RANGE\\_x\\_DNS\\_SERVERS](#) (Seite 140)

DHCP\_EXTRA\_RANGE\_x\_DNS\_SERVER  
DHCP\_EXTRA\_RANGE\_x\_NTP\_SERVER  
DHCP\_RANGE\_x\_DNS\_SERVER1  
DHCP\_RANGE\_x\_DNS\_SERVER2  
DHCP\_RANGE\_x\_NTP\_SERVER  
DHCP\_WINSERVER1  
DHCP\_WINSERVER2

[DHCP\\_RANGE\\_x\\_NTP\\_SERVERS](#) (Seite 140)  
[DHCP\\_RANGE\\_x\\_WINS\\_SERVERS](#) (Seite 140)  
[DHCP\\_WINS\\_SERVERS](#) (Seite 139)

## Package PROXY

### Neue Variablen

IMPROXY\_DOWNSTREAM\_DEV (Seite ??)  
IMPROXY\_ENABLE\_IGMPV3 (Seite ??)  
IMPROXY\_ENABLE\_MLD (Seite ??)  
IMPROXY\_UPSTREAM\_DEV (Seite ??)  
OPT\_IMPROXY (Seite ??)  
SIPROXD\_N (Seite ??)  
SIPROXD\_x\_ALLOW\_REG\_N (Seite ??)  
SIPROXD\_x\_ALLOW\_REG\_x (Seite ??)  
SIPROXD\_x\_DEV\_IN (Seite ??)  
SIPROXD\_x\_DEV\_OUT (Seite ??)  
SIPROXD\_x\_RTP\_PORT\_MAX (Seite ??)  
SIPROXD\_x\_RTP\_PORT\_MIN (Seite ??)  
SIPROXD\_x\_SIP\_PORT (Seite ??)  
SIPROXD\_x\_TRANSPARENT (Seite ??)  
SIPROXD\_x\_USER\_N (Seite ??)  
SIPROXD\_x\_USER\_x\_NAME (Seite ??)  
SIPROXD\_x\_USER\_x\_PASS (Seite ??)

### Gelöschte Variablen

## Package TOOLS

### Neue Variablen

[OPT\\_BMON](#) (Seite 266)

### Gelöschte Variablen

## B.23. Unterschiede Version 4.0.0 und 3.10.16

## Package ADVANCED\_NETWORKING

### Neue Variablen

DSA\_N (Seite ??)  
DSA\_x\_BRIDGE (Seite ??)  
DSA\_x\_DEV (Seite ??)  
DSA\_x\_GROUP\_N (Seite ??)  
DSA\_x\_GROUP\_x\_PORT\_N (Seite ??)  
DSA\_x\_GROUP\_x\_PORT\_x\_DEV (Seite ??)  
OPT\_DSA (Seite ??)

### Gelöschte Variablen

## Package CIRCUITS

### Neue Variablen

CIRC\_x\_NET\_IPV4\_ADDRESS (Seite ??)

### Gelöschte Variablen

CIRC\_x\_NET\_ADDRESS\_IPV4

## B. Anhänge der optionalen Pakete

CIRC\_x\_NET\_IPV6\_ADDRESS (Seite ??)                      CIRC\_x\_NET\_ADDRESS\_IPV6  
CIRC\_x\_NET\_IPV6\_ADVERTISE\_PREFIX (Seite ??)  
CIRC\_x\_NET\_IPV6\_ADVERTISE\_PREFIX\_ON\_LINK  
(Seite ??)  
CIRC\_x\_NET\_IPV6\_ADVERTISE\_PREFIX\_  
PREFERRED\_LIFETIME (Seite ??)  
CIRC\_x\_NET\_IPV6\_ADVERTISE\_PREFIX\_VALID\_  
LIFETIME (Seite ??)

### Package DNS\_DHCP

#### Neue Variablen

CIRC\_x\_NET\_IPV6\_ADVERTISE\_DNS (Seite ??)  
[DHCP\\_DNS\\_SERVERS](#) (Seite 139)  
[DHCP\\_EXTRA\\_RANGE\\_x\\_DNS\\_SERVERS](#) (Seite 141)  
[DHCP\\_EXTRA\\_RANGE\\_x\\_NTP\\_SERVERS](#) (Seite 141)  
[DHCP\\_EXTRA\\_RANGE\\_x\\_WINS\\_SERVERS](#) (Seite 141)  
[DHCP\\_NTP\\_SERVERS](#) (Seite 139)  
[DHCP\\_RANGE\\_x\\_DNS\\_SERVERS](#) (Seite 140)  
[DHCP\\_RANGE\\_x\\_NTP\\_SERVERS](#) (Seite 140)  
[DHCP\\_RANGE\\_x\\_WINS\\_SERVERS](#) (Seite 140)  
[DHCP\\_WINS\\_SERVERS](#) (Seite 139)

#### Gelöschte Variablen

DHCP\_EXTRA\_RANGE\_x\_DNS\_SERVER  
DHCP\_EXTRA\_RANGE\_x\_NTP\_SERVER  
DHCP\_RANGE\_x\_DNS\_SERVER1  
DHCP\_RANGE\_x\_DNS\_SERVER2  
DHCP\_RANGE\_x\_NTP\_SERVER  
DHCP\_WINSERVER1  
DHCP\_WINSERVER2

### Package PROXY

#### Neue Variablen

IMPROXY\_DOWNSTREAM\_DEV (Seite ??)  
IMPROXY\_ENABLE\_IGMPV3 (Seite ??)  
IMPROXY\_ENABLE\_MLD (Seite ??)  
IMPROXY\_UPSTREAM\_DEV (Seite ??)  
OPT\_IMPROXY (Seite ??)  
SIPROXD\_N (Seite ??)  
SIPROXD\_x\_ALLOW\_REG\_N (Seite ??)  
SIPROXD\_x\_ALLOW\_REG\_x (Seite ??)  
SIPROXD\_x\_DEV\_IN (Seite ??)  
SIPROXD\_x\_DEV\_OUT (Seite ??)  
SIPROXD\_x\_RTP\_PORT\_MAX (Seite ??)  
SIPROXD\_x\_RTP\_PORT\_MIN (Seite ??)  
SIPROXD\_x\_SIP\_PORT (Seite ??)  
SIPROXD\_x\_TRANSPARENT (Seite ??)  
SIPROXD\_x\_USER\_N (Seite ??)  
SIPROXD\_x\_USER\_x\_NAME (Seite ??)  
SIPROXD\_x\_USER\_x\_PASS (Seite ??)

#### Gelöschte Variablen

### Package TOOLS

#### Neue Variablen

[OPT\\_BMON](#) (Seite 266)

#### Gelöschte Variablen

## B.24. Unterschiede Version 4.0.0 und 3.10.17

## Package ADVANCED\_NETWORKING

### Neue Variablen

DSA\_N (Seite ??)  
DSA\_x\_BRIDGE (Seite ??)  
DSA\_x\_DEV (Seite ??)  
DSA\_x\_GROUP\_N (Seite ??)  
DSA\_x\_GROUP\_x\_PORT\_N (Seite ??)  
DSA\_x\_GROUP\_x\_PORT\_x\_DEV (Seite ??)  
OPT\_DSA (Seite ??)

### Gelöschte Variablen

## Package PROXY

### Neue Variablen

SIPROXD\_N (Seite ??)  
SIPROXD\_x\_ALLOW\_REG\_N (Seite ??)  
SIPROXD\_x\_ALLOW\_REG\_x (Seite ??)  
SIPROXD\_x\_DEV\_IN (Seite ??)  
SIPROXD\_x\_DEV\_OUT (Seite ??)  
SIPROXD\_x\_RTP\_PORT\_MAX (Seite ??)  
SIPROXD\_x\_RTP\_PORT\_MIN (Seite ??)  
SIPROXD\_x\_SIP\_PORT (Seite ??)  
SIPROXD\_x\_TRANSPARENT (Seite ??)  
SIPROXD\_x\_USER\_N (Seite ??)  
SIPROXD\_x\_USER\_x\_NAME (Seite ??)  
SIPROXD\_x\_USER\_x\_PASS (Seite ??)

### Gelöschte Variablen

## Package TOOLS

### Neue Variablen

[OPT\\_BMON](#) (Seite 266)

### Gelöschte Variablen

## B.25. Unterschiede Version 4.0.0 und 3.10.18

## Package ADVANCED\_NETWORKING

### Neue Variablen

DSA\_N (Seite ??)  
DSA\_x\_BRIDGE (Seite ??)  
DSA\_x\_DEV (Seite ??)  
DSA\_x\_GROUP\_N (Seite ??)  
DSA\_x\_GROUP\_x\_PORT\_N (Seite ??)  
DSA\_x\_GROUP\_x\_PORT\_x\_DEV (Seite ??)

### Gelöschte Variablen

## Package PROXY

## Neue Variablen

SIPROXD\_N (Seite ??)  
SIPROXD\_x\_ALLOW\_REG\_N (Seite ??)  
SIPROXD\_x\_ALLOW\_REG\_x (Seite ??)  
SIPROXD\_x\_DEV\_IN (Seite ??)  
SIPROXD\_x\_DEV\_OUT (Seite ??)  
SIPROXD\_x\_RTP\_PORT\_MAX (Seite ??)  
SIPROXD\_x\_RTP\_PORT\_MIN (Seite ??)  
SIPROXD\_x\_SIP\_PORT (Seite ??)  
SIPROXD\_x\_TRANSPARENT (Seite ??)  
SIPROXD\_x\_USER\_N (Seite ??)  
SIPROXD\_x\_USER\_x\_NAME (Seite ??)  
SIPROXD\_x\_USER\_x\_PASS (Seite ??)

## Gelöschte Variablen

## Package TOOLS

## Neue Variablen

[OPT\\_BMON](#) (Seite [266](#))

## Gelöschte Variablen



# Abbildungsverzeichnis

3.1. Struktur des Paketfilters . . . . .	50
3.2. Verzeichnisstruktur fli4l . . . . .	59
4.1. VPN-Konfigurationsbeispiel — Tunnel zwischen zwei Routern . . . . .	197
4.2. fli4l config Directory mit OpenVPN *.secret Dateien . . . . .	201
4.3. Verbindungsübersicht . . . . .	217
4.4. Detailansicht einer Verbindung (Keymanagement) . . . . .	218
4.5. Beispiel 1 . . . . .	255
4.6. Beispiel 2 . . . . .	256
4.7. Beispiel 3 . . . . .	259
4.8. Verzeichnisstruktur fli4l . . . . .	262
5.1. Einstellungen . . . . .	310
5.2. Einstellungen für Remoteupdate . . . . .	311
5.3. Einstellungen für HD-pre-install . . . . .	312

# Tabellenverzeichnis

3.1. Übersicht über die (Zusatz-)Pakete . . . . .	19
3.2. Automatische Einstellung der maximalen Verbindungsanzahl . . . . .	34
3.3. Typen von Netzwerkpräfixen . . . . .	47
3.4. Aktionen in Paketfilterregeln . . . . .	51
3.5. Quell- und Zieleinschränkungen in Paketfilterregeln . . . . .	52
3.6. Zustandseinschränkungen in Paketfilterregeln . . . . .	55
3.7. Im Lieferumfang von fli4l enthaltene Schablonen . . . . .	58
3.8. Verfügbare Conntrack-Helfer im Paketfilter . . . . .	76
3.9. Format der Imond-Logdatei . . . . .	85
3.10. Verfügbare Circuit-Typen . . . . .	87
3.11. Circuit-Zustände . . . . .	94
3.12. Circuit-Zustandsübergänge . . . . .	95
3.13. Verfügbare Wählmodi . . . . .	96
3.14. fli4lctrl-Befehle . . . . .	99
3.15. fli4lctrl-Statusbefehle . . . . .	100
4.1. Verfügbare LAN-Adapter-Treiber in Linux 5.4 . . . . .	110
4.2. Verfügbare WLAN-Adapter-Treiber in Linux 5.4 . . . . .	111
4.3. Werte für BRIDGE_DEV_x_DEV_x_PATHCOST in Abhängigkeit von der Bandbreite . . . . .	123
4.4. Unterstützte interne DSL-Modems . . . . .	149
4.5. Beispiel für die Konfiguration des Setup-Mediums . . . . .	159
4.6. Beispiel für eine Installation nach Typ A oder B . . . . .	160
4.8. In OpenVPN verfügbare Verschlüsselungsmethoden . . . . .	206
4.9. In OpenVPN verfügbare Prüfsummenmethoden . . . . .	207
4.10. Aktionen der OpenVPN-Webgui . . . . .	218
4.11. Unterschiedliche MTU Parameter der unterschiedlichen OpenVPN Versionen. . . . .	220
4.12. Unterschiedliche MTU Parameter der fli4l-Router Versionen. . . . .	220
4.13. OpenVPN Konfiguration mit 2 fli4l-Routern . . . . .	221
4.14. OpenVPN Konfiguration mit 2 fli4l-Routern deren Netzwerk über eine Funkver- bindung gebridgt wird. . . . .	221
4.15. OpenVPN Konfiguration mit 2 fli4l-Routern deren Netzwerk über eine Funkver- bindung gebridgt wird. Die Konfiguration der Bridge in advanced_networking. . . . .	222
4.16. OpenVPN Konfiguration mit 2 fli4l-Routern deren Netzwerk über eine Funkver- bindung gebridgt wird. Die Konfiguration der Bridge in der Basiskonfiguration (base.txt). . . . .	222
4.17. OpenVPN Konfiguration mit einem Windowsrechner über GPRS. . . . .	223
4.18. OpenVPN Absicherung eines WLAN. . . . .	224
4.19. Verfügbare PPP-Typen . . . . .	227
4.20. Mit CIRC_x_PPP_COMP_MPPE_KEY_LEN konfigurierbare MPPE-Schlüssellängen . . . . .	235

4.21. Arten der PPPoE-Paketerzeugung . . . . .	243
4.22. Einwahldaten einiger deutscher Netzbetreiber/Provider . . . . .	277
4.23. Arten der GRE-Paketerzeugung . . . . .	280
4.24. Einstellungen für Provider, die PPTP nutzen . . . . .	281
8.1. Parameter für <code>mkfli4l</code> . . . . .	342
8.2. Optionen für Dateien . . . . .	346
8.3. Logische Ausdrücke . . . . .	369
8.4. Funktionen des <code>cgi-helper</code> -Skriptes . . . . .	384

# Index

ADDMODULES, [435](#)  
AUTOMOUNT\_UNKNOWN, [162](#)  
AUTOMOUNT\_UNKNOWN\_OPTS, [162](#)  
  
base.txt, [19](#)  
BCRELAY\_N, [113](#)  
BCRELAY\_x\_IF\_N, [113](#)  
BCRELAY\_x\_IF\_x, [113](#)  
BEEP, [35](#), [435](#)  
Beispiel-Datei(base.txt), [19](#)  
BONDING\_DEV\_N, [114](#)  
BONDING\_DEV\_x\_ARP\_INTERVAL,  
    [117](#)  
BONDING\_DEV\_x\_ARP\_IP\_-  
    TARGET\_N, [117](#)  
BONDING\_DEV\_x\_ARP\_IP\_-  
    TARGET\_x, [117](#)  
BONDING\_DEV\_x\_DEV\_N, [116](#)  
BONDING\_DEV\_x\_DEV\_x, [116](#)  
BONDING\_DEV\_x\_DEVNAME, [114](#)  
BONDING\_DEV\_x\_DOWNDELAY, [116](#)  
BONDING\_DEV\_x\_LACP\_RATE, [117](#)  
BONDING\_DEV\_x\_MAC, [116](#)  
BONDING\_DEV\_x\_MIIMON, [116](#)  
BONDING\_DEV\_x\_MODE, [114](#)  
BONDING\_DEV\_x\_PRIMARY, [117](#)  
BONDING\_DEV\_x\_UPDELAY, [116](#)  
BONDING\_DEV\_x\_USE\_CARRIER,  
    [116](#)  
BOOT\_TYPE, [29](#), [435](#)  
BOOTMENU\_TIME, [30](#), [435](#)  
BRIDGE\_DEV\_BOOTDELAY, [120](#)  
BRIDGE\_DEV\_N, [120](#)  
BRIDGE\_DEV\_x\_AGING, [121](#)  
BRIDGE\_DEV\_x\_DEV\_N, [120](#)  
BRIDGE\_DEV\_x\_DEV\_x\_DEV, [120](#)  
BRIDGE\_DEV\_x\_DEV\_x\_-  
    PATHCOST, [122](#)  
  
BRIDGE\_DEV\_x\_DEV\_x\_PORT\_-  
    PRIORITY, [122](#)  
BRIDGE\_DEV\_x\_DEVNAME, [120](#)  
BRIDGE\_DEV\_x\_FORWARD\_DELAY,  
    [121](#)  
BRIDGE\_DEV\_x\_GARBAGE\_-  
    COLLECTION\_INTERVAL,  
    [121](#)  
BRIDGE\_DEV\_x\_HELLO, [122](#)  
BRIDGE\_DEV\_x\_MAX\_MESSAGE\_-  
    AGE, [122](#)  
BRIDGE\_DEV\_x\_NAME, [120](#)  
BRIDGE\_DEV\_x\_PRIORITY, [121](#)  
BRIDGE\_DEV\_x\_STP, [121](#)  
BUG\_CHECK, [435](#)  
BUILDDIR, [313](#)  
  
CERT\_X509\_MOZILLA, [128](#)  
CHRONY\_BIOS\_TIME, [437](#), [445](#), [447](#),  
    [450](#), [452](#), [454](#), [456](#)  
CHRONY\_LOG, [130](#)  
CHRONY\_TIMESERVER\_N, [130](#)  
CHRONY\_TIMESERVER\_x, [130](#)  
CHRONY\_TIMESERVICE, [130](#)  
CIRC\_CLASS\_N, [97](#)  
CIRC\_CLASS\_x\_NAME, [97](#)  
CIRC\_N, [87](#)  
CIRC\_ONLINE, [102](#)  
CIRC\_x\_BUNDLE, [93](#)  
CIRC\_x\_CHARGEINT, [91](#)  
CIRC\_x\_CLASS\_N, [92](#)  
CIRC\_x\_CLASS\_y, [92](#)  
CIRC\_x\_DEBUG, [92](#)  
CIRC\_x\_DEPS, [92](#)  
CIRC\_x\_DHCP\_ACCEPT\_CSR, [145](#)  
CIRC\_x\_DHCP\_DAEMON, [144](#)  
CIRC\_x\_DHCP\_DEV, [144](#)  
CIRC\_x\_DHCP\_HOSTNAME, [144](#)

- CIRC\_x\_DHCP\_STARTDELAY, [144](#)
- CIRC\_x\_DIALMODE, [88](#)
- CIRC\_x\_ENABLED, [88](#)
- CIRC\_x\_HUP\_TIMEOUT, [91](#)
- CIRC\_x\_NAME, [87](#)
- CIRC\_x\_NET\_ADDRESS\_IPV4, [444](#),  
[447](#), [449](#), [452](#), [454](#), [456](#), [457](#),  
[459–461](#)
- CIRC\_x\_NET\_ADDRESS\_IPV6, [444](#),  
[447](#), [449](#), [452](#), [454](#), [456](#), [457](#), [459](#),  
[460](#), [462](#)
- CIRC\_x\_NETS\_IPV4\_N, [88](#)
- CIRC\_x\_NETS\_IPV4\_y, [88](#)
- CIRC\_x\_NETS\_IPV6\_N, [88](#)
- CIRC\_x\_NETS\_IPV6\_y, [88](#)
- CIRC\_x\_PPP\_COMP\_BSDCOMP, [231](#)
- CIRC\_x\_PPP\_COMP\_BSDCOMP\_-  
LEVEL, [231](#)
- CIRC\_x\_PPP\_COMP\_DEFLATE, [232](#)
- CIRC\_x\_PPP\_COMP\_DEFLATE\_-  
LEVEL, [232](#)
- CIRC\_x\_PPP\_COMP\_LZSCOMP, [232](#)
- CIRC\_x\_PPP\_COMP\_LZSCOMP\_-  
NHIST, [234](#)
- CIRC\_x\_PPP\_COMP\_MPPE, [234](#)
- CIRC\_x\_PPP\_COMP\_MPPE\_KEY\_-  
LEN, [235](#)
- CIRC\_x\_PPP\_DECOMP\_BSDCOMP,  
[231](#)
- CIRC\_x\_PPP\_DECOMP\_BSDCOMP\_-  
LEVEL, [231](#)
- CIRC\_x\_PPP\_DECOMP\_DEFLATE,  
[232](#)
- CIRC\_x\_PPP\_DECOMP\_DEFLATE\_-  
LEVEL, [232](#)
- CIRC\_x\_PPP\_DECOMP\_LZSCOMP,  
[232](#)
- CIRC\_x\_PPP\_DECOMP\_LZSCOMP\_-  
NHIST, [234](#)
- CIRC\_x\_PPP\_DSLMODEM\_-  
PROVIDER, [149](#)
- CIRC\_x\_PPP\_DSLMODEM\_TYPE,  
[149](#)
- CIRC\_x\_PPP\_ETHERNET\_DEV, [242](#)
- CIRC\_x\_PPP\_ETHERNET\_-  
SERVER\_DEV, [244](#)
- CIRC\_x\_PPP\_ETHERNET\_-  
SERVER\_SESSIONS, [244](#)
- CIRC\_x\_PPP\_ETHERNET\_-  
SERVER\_TYPE, [244](#)
- CIRC\_x\_PPP\_ETHERNET\_TYPE, [243](#)
- CIRC\_x\_PPP\_FILTER, [228](#)
- CIRC\_x\_PPP\_FILTER\_EXPR, [229](#)
- CIRC\_x\_PPP\_LOCALIP, [228](#)
- CIRC\_x\_PPP\_LOCALIP6, [228](#)
- CIRC\_x\_PPP\_MASTER, [237](#)
- CIRC\_x\_PPP\_MRRU, [237](#)
- CIRC\_x\_PPP\_MRU, [227](#)
- CIRC\_x\_PPP\_MTU, [227](#)
- CIRC\_x\_PPP\_NF\_MSS, [227](#)
- CIRC\_x\_PPP\_PASSWORD, [229](#)
- CIRC\_x\_PPP\_PEER\_AUTH, [230](#)
- CIRC\_x\_PPP\_PPTP\_LOGLEVEL, [281](#)
- CIRC\_x\_PPP\_PPTP\_PEER, [281](#)
- CIRC\_x\_PPP\_PPTP\_REORDER\_-  
TIMEOUT, [281](#)
- CIRC\_x\_PPP\_PPTP\_SERVER\_-  
ALLOW\_FROM\_N, [282](#)
- CIRC\_x\_PPP\_PPTP\_SERVER\_-  
ALLOW\_FROM\_y, [282](#)
- CIRC\_x\_PPP\_PPTP\_SERVER\_-  
LISTEN, [282](#)
- CIRC\_x\_PPP\_PPTP\_SERVER\_-  
SESSIONS, [282](#)
- CIRC\_x\_PPP\_PPTP\_TYPE, [280](#)
- CIRC\_x\_PPP\_REMOTEIP, [228](#)
- CIRC\_x\_PPP\_REMOTEIP6, [228](#)
- CIRC\_x\_PPP\_SERIAL\_DEV, [240](#)
- CIRC\_x\_PPP\_SERIAL\_SERVER\_-  
DEV, [240](#)
- CIRC\_x\_PPP\_SERIAL\_SERVER\_-  
SPEED, [241](#)
- CIRC\_x\_PPP\_SERIAL\_SPEED, [240](#)
- CIRC\_x\_PPP\_TYPE, [227](#)
- CIRC\_x\_PPP\_USERID, [229](#)
- CIRC\_x\_PPP\_VJ, [230](#)
- CIRC\_x\_PPP\_VJCCOMP, [230](#)
- CIRC\_x\_PRIORITY, [89](#)
- CIRC\_x\_PROTOCOLS, [89](#)
- CIRC\_x\_ROUTE\_DEV, [103](#)
- CIRC\_x\_ROUTE\_GATEWAY\_IPV4,  
[103](#)
- CIRC\_x\_ROUTE\_GATEWAY\_IPV6,  
[104](#)

- CIRC\_x\_TIMES, [90](#)
- CIRC\_x\_TUN6IN4\_SIXXS\_LOCALV6, [445](#), [448](#), [450](#), [452](#)
- CIRC\_x\_TUN6IN4\_SIXXS\_-  
PASSWORD, [445](#), [448](#), [450](#), [452](#)
- CIRC\_x\_TUN6IN4\_SIXXS\_PREFIX, [445](#), [448](#), [450](#), [452](#)
- CIRC\_x\_TUN6IN4\_SIXXS\_-  
REMOTEV6, [445](#), [448](#), [450](#), [452](#)
- CIRC\_x\_TUN6IN4\_SIXXS\_TIMEOUT, [445](#), [448](#), [450](#), [452](#)
- CIRC\_x\_TUN6IN4\_SIXXS\_-  
TUNNELID, [445](#), [448](#), [450](#), [453](#)
- CIRC\_x\_TUN6IN4\_SIXXS\_USERID, [445](#), [448](#), [450](#), [453](#)
- CIRC\_x\_TYPE, [87](#)
- CIRC\_x\_UMTS\_APN, [276](#)
- CIRC\_x\_UMTS\_DIALOUT, [276](#)
- CIRC\_x\_UP, [89](#)
- CIRC\_x\_USEPEERDNS, [91](#)
- CIRC\_x\_WAIT, [92](#)
- COMP\_TYPE\_OPT, [33](#), [435](#)
- COMP\_TYPE\_ROOTFS, [32](#)
- COMPRESS\_KERNEL, [433](#), [435](#)
- COMPRESS\_OPT, [433](#), [435](#)
- COMPRESS\_ROOTFS, [433](#), [435](#)
- CONSOLE\_BLANK\_TIME, [35](#), [435](#)
  
- DEBUG\_ENABLE\_CORE, [37](#), [378](#), [435](#)
- DEBUG\_IP, [37](#), [378](#), [435](#)
- DEBUG\_IPTABLES, [37](#)
- DEBUG\_IPUP, [378](#), [435](#)
- DEBUG\_KEEP\_BOOTLOGD, [378](#), [435](#)
- DEBUG\_MDEV, [37](#), [378](#), [435](#)
- DEBUG\_MODULES, [36](#), [435](#)
- DEBUG\_STARTUP, [36](#), [435](#)
- DENY\_ICMP, [433](#), [435](#)
- DEV\_MTU\_N, [119](#)
- DEV\_MTU\_x, [119](#)
- DHCP\_DENY\_MAC\_N, [141](#), [437](#)
- DHCP\_DENY\_MAC\_x, [141](#)
- DHCP\_DNS\_SERVERS, [139](#)
- DHCP\_EXTRA\_RANGE\_N, [141](#), [437](#)
- DHCP\_EXTRA\_RANGE\_x\_DEVICE, [141](#)
- DHCP\_EXTRA\_RANGE\_x\_DNS\_SERVER, [437](#), [445](#), [448](#), [450](#), [452](#), [454](#), [456](#), [458–460](#), [462](#)
- DHCP\_EXTRA\_RANGE\_x\_DNS\_SERVERS, [141](#)
- DHCP\_EXTRA\_RANGE\_x\_END, [141](#)
- DHCP\_EXTRA\_RANGE\_x\_-  
GATEWAY, [141](#)
- DHCP\_EXTRA\_RANGE\_x\_MTU, [141](#)
- DHCP\_EXTRA\_RANGE\_x\_-  
NETMASK, [141](#)
- DHCP\_EXTRA\_RANGE\_x\_NTP\_SERVER, [437](#), [445](#), [448](#), [450](#), [452](#), [454](#), [456](#), [458–460](#), [462](#)
- DHCP\_EXTRA\_RANGE\_x\_NTP\_SERVERS, [141](#)
- DHCP\_EXTRA\_RANGE\_x\_START, [141](#)
- DHCP\_EXTRA\_RANGE\_x\_WINS\_SERVERS, [141](#)
- DHCP\_LEASES\_DIR, [139](#)
- DHCP\_LEASES\_VOLATILE, [139](#)
- DHCP\_LS\_TIME\_DYN, [138](#)
- DHCP\_LS\_TIME\_FIX, [139](#)
- DHCP\_MAX\_LS\_TIME\_DYN, [139](#)
- DHCP\_MAX\_LS\_TIME\_FIX, [139](#)
- DHCP\_NTP\_SERVERS, [139](#)
- DHCP\_OPTION\_WPAD, [139](#)
- DHCP\_OPTION\_WPAD\_URL, [139](#)
- DHCP\_RANGE\_N, [140](#), [437](#)
- DHCP\_RANGE\_x\_DNS\_DOMAIN, [140](#)
- DHCP\_RANGE\_x\_DNS\_SERVER1, [437](#), [445](#), [448](#), [450](#), [452](#), [454](#), [456](#), [458–460](#), [462](#)
- DHCP\_RANGE\_x\_DNS\_SERVER2, [437](#), [445](#), [448](#), [450](#), [452](#), [454](#), [456](#), [458–460](#), [462](#)
- DHCP\_RANGE\_x\_DNS\_SERVERS, [140](#)
- DHCP\_RANGE\_x\_END, [140](#)
- DHCP\_RANGE\_x\_GATEWAY, [140](#)
- DHCP\_RANGE\_x\_MTU, [140](#)
- DHCP\_RANGE\_x\_NET, [140](#)
- DHCP\_RANGE\_x\_NTP\_SERVER, [437](#), [445](#), [448](#), [450](#), [452](#), [454](#), [456](#), [458–460](#), [462](#)

- DHCP\_RANGE\_x\_NTP\_SERVERS, 140
- DHCP\_RANGE\_x\_OPTION\_N, 141, 437
- DHCP\_RANGE\_x\_OPTION\_WPAD, 140
- DHCP\_RANGE\_x\_OPTION\_WPAD\_URL, 140
- DHCP\_RANGE\_x\_OPTION\_x, 141
- DHCP\_RANGE\_x\_PXE\_FILENAME, 142
- DHCP\_RANGE\_x\_PXE\_OPTIONS, 142
- DHCP\_RANGE\_x\_PXE\_SERVERIP, 142
- DHCP\_RANGE\_x\_PXE\_SERVERNAME, 142
- DHCP\_RANGE\_x\_START, 140
- DHCP\_RANGE\_x\_WINS\_SERVERS, 140
- DHCP\_TYPE, 138
- DHCP\_VERBOSE, 138
- DHCP\_WINS\_SERVERS, 139
- DHCP\_WINSERVER1, 445, 448, 450, 452, 455, 456, 458–460, 462
- DHCP\_WINSERVER2, 445, 448, 450, 452, 455, 456, 458–460, 462
- DHCP\_WINSERVER\_1, 437
- DHCP\_WINSERVER\_2, 437
- DHCPRELAY\_IF\_N, 142, 437
- DHCPRELAY\_IF\_x, 142
- DHCPRELAY\_SERVER, 142
- DIALMODE, 96, 433
- DMZ\_LOG, 433, 435
- DMZ\_NAT, 433, 435
- DMZ\_ORANGE\_RED\_N, 433, 435
- DMZ\_ORANGE\_RED\_x, 433, 435
- DMZ\_ORANGE\_ROUTER\_N, 433, 435
- DMZ\_ORANGE\_ROUTER\_x, 433, 435
- DMZ\_RED\_DEV, 433, 435
- DNS\_AUTHORITATIVE, 135
- DNS\_AUTHORITATIVE\_LISTEN, 136
- DNS\_AUTHORITATIVE\_NS, 136
- DNS\_BIND\_INTERFACES, 132
- DNS\_BOGUS\_PRIV, 134
- DNS\_FILTERWIN2K, 134
- DNS\_FORBIDDEN\_N, 133, 437
- DNS\_FORBIDDEN\_x, 133
- DNS\_FORWARD\_LOCAL, 135
- DNS\_FORWARD\_PRIV\_x, 134
- DNS\_FORWARDERS, 83, 435
- DNS\_LISTEN\_N, 132
- DNS\_LISTEN\_x, 132
- DNS\_LISTENIP\_N, 437
- DNS\_LISTENIP\_x, 437
- DNS\_LOCAL\_HOST\_CACHE\_TTL, 135
- DNS\_MX\_SERVER, 133
- DNS\_REBINDOK\_N, 138, 437
- DNS\_REBINDOK\_x\_DOMAIN, 138
- DNS\_REDIRECT\_N, 133, 437
- DNS\_REDIRECT\_x, 133
- DNS\_REDIRECT\_x\_IP, 133
- DNS\_SPECIAL\_N, 437
- DNS\_SPECIAL\_x\_DNSIP, 438
- DNS\_SPECIAL\_x\_DOMAIN, 438
- DNS\_SPECIAL\_x\_NETWORK, 438
- DNS\_SUPPORT\_IPV6, 135
- DNS\_VERBOSE, 133
- DNS\_ZONE\_DELEGATION\_N, 136
- DNS\_ZONE\_DELEGATION\_x, 136
- DNS\_ZONE\_DELEGATION\_x\_DOMAIN, 136
- DNS\_ZONE\_DELEGATION\_x\_NETWORK, 136
- DNS\_ZONE\_DELEGATION\_x\_UPSTREAM\_SERVER\_x, 136
- DNS\_ZONE\_DELEGATION\_x\_UPSTREAM\_SERVER\_x\_IP, 136
- DNS\_ZONE\_DELEGATION\_x\_UPSTREAM\_SERVER\_x\_querySOURCEIP, 136
- DNS\_ZONE\_NETWORK\_N, 136
- DNS\_ZONE\_NETWORK\_x, 136
- DOMAIN\_NAME, 82, 435
- DYNDNS\_ALLOW\_SSL, 155, 438
- DYNDNS\_DEBUG\_PROVIDER, 156
- DYNDNS\_LOGINTIME, 155
- DYNDNS\_LOOKUP\_NAMES, 155
- DYNDNS\_N, 154
- DYNDNS\_SAVE\_OUTPUT, 154
- DYNDNS\_x\_CIRCUIT, 154, 438
- DYNDNS\_x\_EXT\_IP, 438

DYNDNS\_x\_EXT\_IPV4, [155](#)  
 DYNDNS\_x\_EXT\_IPV6, [155](#)  
 DYNDNS\_x\_HOSTNAME, [154](#)  
 DYNDNS\_x\_LOGIN, [155](#)  
 DYNDNS\_x\_PASSWORD, [154](#)  
 DYNDNS\_x\_PROVIDER, [154](#)  
 DYNDNS\_x\_RENEW, [155](#), [438](#)  
 DYNDNS\_x\_UPDATEHOST, [154](#), [438](#)  
 DYNDNS\_x\_USER, [154](#), [438](#)  
  
 EASYCRON\_MAIL, [156](#)  
 EASYCRON\_N, [156](#)  
 EASYCRON\_x\_COMMAND, [156](#)  
 EASYCRON\_x\_CUSTOM, [156](#)  
 EASYCRON\_x\_TIME, [157](#)  
 ETHTOOL\_DEV\_N, [126](#)  
 ETHTOOL\_DEV\_x, [126](#)  
 ETHTOOL\_DEV\_x\_OPTION\_N, [126](#)  
 ETHTOOL\_DEV\_x\_OPTION\_x\_-  
     NAME, [126](#)  
 ETHTOOL\_DEV\_x\_OPTION\_x\_-  
     VALUE, [126](#)  
 EXTMOUNT\_N, [161](#)  
 EXTMOUNT\_x\_FILESYSTEM, [161](#)  
 EXTMOUNT\_x\_HOTPLUG, [161](#)  
 EXTMOUNT\_x\_MOUNTPOINT, [161](#)  
 EXTMOUNT\_x\_OPTIONS, [161](#)  
 EXTMOUNT\_x\_VOLUMEID, [161](#)  
  
 FASTD\_SECRET, [286](#)  
 FILESONLY, [313](#)  
 FLI4L\_UUID, [33](#), [435](#)  
 FORWARD\_DENY\_PORT\_N, [433](#), [435](#)  
 FORWARD\_DENY\_PORT\_x, [433](#), [435](#)  
 FORWARD\_HOST\_N, [433](#), [435](#)  
 FORWARD\_HOST\_WHITE, [433](#), [435](#)  
 FORWARD\_HOST\_x, [433](#), [435](#)  
 ftp, [76](#)  
 FTP\_PF\_ENABLE\_ACTIVE, [267](#)  
  
 h323, [76](#)  
 HDDRV\_N, [164](#)  
 HDDRV\_x, [164](#)  
 HDDRV\_x\_OPTION, [164](#)  
 HDIT\_DATA, [439](#)  
 HDIT\_POWEROFF, [439](#)  
 HDIT\_SIZES, [439](#)  
 HDSLEEP\_TIMEOUT, [164](#)  
  
 HOST\_EXTRA\_N, [132](#), [438](#)  
 HOST\_EXTRA\_x\_IP4, [132](#)  
 HOST\_EXTRA\_x\_IP6, [132](#)  
 HOST\_EXTRA\_x\_NAME, [132](#)  
 HOST\_N, [131](#), [438](#)  
 HOST\_x\_ALIAS\_N, [131](#), [438](#)  
 HOST\_x\_ALIAS\_x, [131](#)  
 HOST\_x\_DHCPTYP, [131](#)  
 HOST\_x\_DOMAIN, [131](#)  
 HOST\_x\_IP4, [131](#)  
 HOST\_x\_IP6, [131](#)  
 HOST\_x\_MAC, [131](#)  
 HOST\_x\_MAC2, [131](#)  
 HOST\_x\_NAME, [131](#)  
 HOST\_x\_PXE\_FILENAME, [142](#)  
 HOST\_x\_PXE\_OPTIONS, [142](#)  
 HOST\_x\_PXE\_SERVERIP, [142](#)  
 HOST\_x\_PXE\_SERVERNAME, [142](#)  
 HOSTNAME, [28](#), [435](#)  
 HOSTNAME\_ALIAS\_N, [83](#), [433](#), [435](#)  
 HOSTNAME\_ALIAS\_x, [83](#), [435](#)  
 HOSTNAME\_IP, [83](#), [435](#)  
 HOSTNAME\_IP6, [45](#), [439](#)  
 HTTPD\_ARPING, [166](#)  
 HTTPD\_ARPING\_IGNORE\_N, [166](#)  
 HTTPD\_ARPING\_IGNORE\_x, [166](#)  
 HTTPD\_GUI\_LANG, [165](#)  
 HTTPD\_GUI\_SKIN, [439](#)  
 HTTPD\_LISTENIP, [165](#)  
 HTTPD\_PORT, [165](#)  
 HTTPD\_PORTFW, [166](#)  
 HTTPD\_USER, [417](#)  
 HTTPD\_USER\_N, [166](#)  
 HTTPD\_USER\_x\_PASSWORD, [166](#)  
 HTTPD\_USER\_x\_RIGHTS, [166](#)  
 HTTPD\_USER\_x\_USERNAME, [166](#)  
 HW\_DETECT\_AT\_BOOTTIME, [273](#)  
 HWSUPP\_BOOT\_LED, [173](#)  
 HWSUPP\_BUTTON\_N, [173](#)  
 HWSUPP\_BUTTON\_x, [173](#)  
 HWSUPP\_BUTTON\_x\_DEVICE, [173](#)  
 HWSUPP\_BUTTON\_x\_PARAM, [174](#)  
 HWSUPP\_CPUFREQ, [171](#)  
 HWSUPP\_CPUFREQ\_GOVERNOR,  
     [171](#)  
 HWSUPP\_DRIVER\_N, [175](#)  
 HWSUPP\_DRIVER\_x, [175](#)



- HWSUPP\_I2C\_N, [175](#)
- HWSUPP\_I2C\_x\_ADDRESS, [175](#)
- HWSUPP\_I2C\_x\_BUS, [175](#)
- HWSUPP\_I2C\_x\_DEVICE, [175](#)
- HWSUPP\_LED\_N, [171](#)
- HWSUPP\_LED\_PARAM, [172](#)
- HWSUPP\_LED\_x, [171](#)
- HWSUPP\_LED\_x\_DEVICE, [172](#)
- HWSUPP\_TYPE, [170](#)
- HWSUPP\_WATCHDOG, [171](#)
  
- IGNORE\_IP\_NET\_WARNING, [435](#)
- IMOND\_ADMIN\_PASS, [84](#), [433](#)
- IMOND\_BEEP, [85](#), [433](#)
- IMOND\_DIAL, [85](#), [434](#)
- IMOND\_ENABLE, [85](#), [434](#)
- IMOND\_LED, [84](#), [434](#)
- IMOND\_LOG, [85](#), [434](#)
- IMOND\_LOGDIR, [85](#), [434](#)
- IMOND\_PASS, [84](#), [434](#)
- IMOND\_PORT, [84](#), [434](#)
- IMOND\_REBOOT, [85](#), [434](#)
- IMOND\_ROUTE, [85](#), [434](#)
- IMOND\_USE\_ORIG, [434](#), [435](#)
- INPUT\_ACCEPT\_PORT\_N, [434](#), [435](#)
- INPUT\_ACCEPT\_PORT\_x, [434](#), [435](#)
- INPUT\_POLICY, [434](#), [435](#)
- IP\_CONNTRACK\_MAX, [33](#), [435](#)
- IP\_DYN\_ADDR, [103](#), [434](#)
- IP\_NET\_N, [41](#), [434](#), [435](#)
- IP\_NET\_x, [41](#), [435](#)
- IP\_NET\_x\_COMMENT, [43](#), [435](#)
- IP\_NET\_x\_DEV, [42](#), [435](#)
- IP\_NET\_x\_MAC, [42](#), [435](#)
- IP\_NET\_x\_NAME, [43](#), [435](#)
- IP\_NET\_x\_TYPE, [43](#), [434](#), [436](#)
- IP\_ROUTE\_N, [48](#), [434](#), [436](#)
- IP\_ROUTE\_x, [48](#), [436](#)
- IPV6\_NET\_N, [45](#), [439](#)
- IPV6\_NET\_x, [45](#), [439](#)
- IPV6\_NET\_x\_ADVERTISE, [46](#), [439](#)
- IPV6\_NET\_x\_ADVERTISE\_DNS, [46](#), [439](#)
- IPV6\_NET\_x\_DEV, [45](#), [439](#)
- IPV6\_NET\_x\_DHCP, [439](#)
- IPV6\_NET\_x\_NAME, [46](#), [439](#)
- IPV6\_NET\_x\_TUNNEL, [439](#)
- IPV6\_ROUTE\_N, [49](#), [439](#)
- IPV6\_ROUTE\_x, [49](#), [439](#)
- IPV6\_TUNNEL\_N, [176](#), [439](#)
- IPV6\_TUNNEL\_x\_DEFAULT, [176](#), [439](#)
- IPV6\_TUNNEL\_x\_DEV, [178](#), [439](#)
- IPV6\_TUNNEL\_x\_LOCALV4, [177](#), [439](#)
- IPV6\_TUNNEL\_x\_LOCALV6, [178](#), [439](#)
- IPV6\_TUNNEL\_x\_MTU, [178](#), [439](#)
- IPV6\_TUNNEL\_x\_PASSWORD, [178](#), [439](#)
- IPV6\_TUNNEL\_x\_PREFIX, [177](#), [439](#)
- IPV6\_TUNNEL\_x\_REMOTEV4, [177](#), [439](#)
- IPV6\_TUNNEL\_x\_REMOTEV6, [178](#), [439](#)
- IPV6\_TUNNEL\_x\_TIMEOUT, [179](#), [439](#)
- IPV6\_TUNNEL\_x\_TUNNELID, [179](#), [439](#)
- IPV6\_TUNNEL\_x\_TYPE, [176](#), [439](#)
- IPV6\_TUNNEL\_x\_USERID, [178](#), [439](#)
- irc, [76](#)
- ISDN\_%\_IO, [180](#)
- ISDN\_%\_IO0, [180](#)
- ISDN\_%\_IO1, [180](#)
- ISDN\_%\_IP, [182](#)
- ISDN\_%\_MEM, [180](#)
- ISDN\_%\_PORT, [182](#)
- ISDN\_%\_TYPE, [180](#)
- ISDN\_CIRC\_N, [184](#)
- ISDN\_CIRC\_x\_AUTH, [190](#)
- ISDN\_CIRC\_x\_BANDWIDTH, [185](#)
- ISDN\_CIRC\_x\_BUNDLING, [185](#)
- ISDN\_CIRC\_x\_CALLBACK, [189](#)
- ISDN\_CIRC\_x\_CBDELAY, [189](#)
- ISDN\_CIRC\_x\_CBNUMBER, [189](#)
- ISDN\_CIRC\_x\_CHARGEINT, [191](#)
- ISDN\_CIRC\_x\_CLAMP\_MSS, [187](#)
- ISDN\_CIRC\_x\_DEBUG, [190](#)
- ISDN\_CIRC\_x\_DIALIN, [189](#)
- ISDN\_CIRC\_x\_DIALOUT, [188](#)
- ISDN\_CIRC\_x\_EAZ, [190](#)
- ISDN\_CIRC\_x\_FRAMECOMP, [187](#)
- ISDN\_CIRC\_x\_HEADERCOMP, [187](#)
- ISDN\_CIRC\_x\_HUP\_TIMEOUT, [190](#)
- ISDN\_CIRC\_x\_LOCAL, [186](#)
- ISDN\_CIRC\_x\_MRU, [187](#)
- ISDN\_CIRC\_x\_MTU, [187](#)
- ISDN\_CIRC\_x\_NAME, [184](#)

- ISDN\_CIRC\_x\_PASS, [188](#)
- ISDN\_CIRC\_x\_REMOTE, [186](#)
- ISDN\_CIRC\_x\_REMOTENAME, [188](#)
- ISDN\_CIRC\_x\_ROUTE\_N, [188](#)
- ISDN\_CIRC\_x\_ROUTE\_X, [188](#)
- ISDN\_CIRC\_x\_SLAVE\_EAZ, [190](#)
- ISDN\_CIRC\_x\_TIMES, [191](#)
- ISDN\_CIRC\_x\_TYPE, [185](#)
- ISDN\_CIRC\_x\_USEPEERDNS, [184](#)
- ISDN\_CIRC\_x\_USER, [188](#)
- ISDN\_DEBUG\_LEVEL, [182](#)
- ISDN\_FILTER, [183](#)
- ISDN\_FILTER\_EXPR, [183](#)
- ISDN\_IO, [440](#), [446](#), [448](#), [450](#)
- ISDN\_IO0, [440](#), [446](#), [448](#), [450](#)
- ISDN\_IO0\_x, [453](#)
- ISDN\_IO1, [440](#), [446](#), [448](#), [450](#)
- ISDN\_IO1\_x, [453](#)
- ISDN\_IO\_x, [453](#)
- ISDN\_IP, [440](#), [446](#), [448](#), [450](#), [453](#)
- ISDN\_IRQ, [440](#), [446](#), [448](#), [450](#)
- ISDN\_IRQ\_x, [453](#)
- ISDN\_LZS\_COMP, [183](#)
- ISDN\_LZS\_DEBUG, [183](#)
- ISDN\_LZS\_TWEAK, [183](#)
- ISDN\_MEM, [440](#), [446](#), [448](#), [450](#)
- ISDN\_MEM\_x, [453](#)
- ISDN\_PORT, [440](#), [446](#), [448](#), [450](#), [453](#)
- ISDN\_TYPE, [440](#), [446](#), [448](#), [450](#)
- ISDN\_TYPE\_x, [453](#)
- ISDN\_VERBOSE\_LEVEL, [182](#)
  
- KERNEL\_BOOT\_OPTION, [32](#), [436](#)
- KERNEL\_VERSION, [32](#), [436](#)
- KEYBOARD\_LOCALE, [38](#), [436](#)
  
- LCD\_VAR\_TEXT\_1, [440](#)
- LCD\_VAR\_TEXT\_2, [440](#)
- LCD\_VAR\_TEXT\_3, [440](#)
- LCD\_VAR\_TEXT\_4, [440](#)
- LIBATA\_DMA, [30](#)
- LIBC\_VERSION, [434](#), [436](#)
- LOCALE, [35](#), [436](#)
- LOG\_BOOT\_SEQ, [378](#), [436](#)
- LOGIP\_LOGDIR, [107](#), [436](#)
  
- MASQ\_MODULE\_N, [434](#), [436](#)
- MASQ\_MODULE\_x, [436](#)
  
- MASQ\_MODULE\_x\_OPTION, [436](#)
- MASQ\_NETWORK, [434](#), [436](#)
- Masquerading, [74](#)
- MKFLI4L\_DEBUG\_OPTION, [314](#)
- MOUNT\_BOOT, [30](#), [436](#)
  
- NET\_DRV\_N, [38](#), [434](#), [436](#)
- NET\_DRV\_x, [39](#), [436](#)
- NET\_DRV\_x\_OPTION, [39](#), [436](#)
- NET\_PREFIX\_x, [46](#)
- NET\_PREFIX\_x\_NAME, [47](#)
- NET\_PREFIX\_x\_STATIC\_IPV4, [47](#)
- NET\_PREFIX\_x\_STATIC\_IPV6, [47](#)
- NET\_PREFIX\_x\_TYPE, [47](#)
- NET\_PREFIX\_x\_ULA\_DEV, [48](#)
  
- OAC\_ALL\_INVISIBLE, [168](#)
- OAC\_BLOCK\_UNKNOWN\_IF\_x, [168](#)
- OAC\_GROUP\_N, [168](#)
- OAC\_GROUP\_x\_BOOTBLOCK, [168](#)
- OAC\_GROUP\_x\_CLIENT\_N, [168](#)
- OAC\_GROUP\_x\_CLIENT\_x, [168](#)
- OAC\_GROUP\_x\_INVISIBLE, [168](#)
- OAC\_GROUP\_x\_NAME, [168](#)
- OAC\_INPUT, [167](#)
- OAC\_LIMITS, [168](#)
- OAC\_MODE, [168](#)
- OAC\_WANDEVICE, [167](#)
- OPENVPN\_DEFAULT\_ALLOW\_-  
ICMPPING, [208](#)
- OPENVPN\_DEFAULT\_CIPHER, [205](#)
- OPENVPN\_DEFAULT\_COMPRESS,  
[206](#)
- OPENVPN\_DEFAULT\_CREATE\_-  
SECRET, [206](#)
- OPENVPN\_DEFAULT\_DIGEST, [207](#)
- OPENVPN\_DEFAULT\_FLOAT, [207](#)
- OPENVPN\_DEFAULT\_FRAGMENT,  
[211](#)
- OPENVPN\_DEFAULT\_KEYSIZE, [208](#)
- OPENVPN\_DEFAULT\_LINK\_MTU,  
[211](#)
- OPENVPN\_DEFAULT\_-  
MANAGEMENT\_LOG\_-  
CACHE, [210](#)
- OPENVPN\_DEFAULT\_MSSFIX, [210](#)

OPENVPN\_DEFAULT\_MUTE\_-  
     REPLAY\_WARNINGS, 210  
 OPENVPN\_DEFAULT\_OPEN\_-  
     OVPNPORT, 208  
 OPENVPN\_DEFAULT\_PF\_DMZ\_-  
     TYPE, 441  
 OPENVPN\_DEFAULT\_PF\_-  
     FORWARD\_LOG, 208  
 OPENVPN\_DEFAULT\_PF\_-  
     FORWARD\_POLICY, 209  
 OPENVPN\_DEFAULT\_PF\_INPUT\_-  
     LOG, 208  
 OPENVPN\_DEFAULT\_PF\_INPUT\_-  
     POLICY, 208  
 OPENVPN\_DEFAULT\_PING, 209  
 OPENVPN\_DEFAULT\_PING\_-  
     RESTART, 209  
 OPENVPN\_DEFAULT\_PROTOCOL,  
     210  
 OPENVPN\_DEFAULT\_RENEG\_SEC,  
     209  
 OPENVPN\_DEFAULT\_RESOLV\_-  
     RETRY, 209  
 OPENVPN\_DEFAULT\_RESTART, 209  
 OPENVPN\_DEFAULT\_SHAPER, 211  
 OPENVPN\_DEFAULT\_START, 210  
 OPENVPN\_DEFAULT\_TUN\_MTU, 211  
 OPENVPN\_DEFAULT\_TUN\_MTU\_-  
     EXTRA, 211  
 OPENVPN\_DEFAULT\_VERBOSE, 210  
 OPENVPN\_EXPERT, 211  
 OPENVPN\_N, 198  
 OPENVPN\_VERSION, 441  
 OPENVPN\_WEBGUI, 216  
 OPENVPN\_x\_ACTIV, 212  
 OPENVPN\_x\_ALLOW\_ICMPING,  
     214  
 OPENVPN\_x\_BRIDGE, 201  
 OPENVPN\_x\_BRIDGE\_COST, 201  
 OPENVPN\_x\_BRIDGE\_PRIORITY,  
     202  
 OPENVPN\_x\_CHECK\_CONFIG, 212  
 OPENVPN\_x\_CHECK\_REPLAY, 216  
 OPENVPN\_x\_CIPHER, 212  
 OPENVPN\_x\_COMPRESS, 212  
 OPENVPN\_x\_CREATE\_SECRET, 212  
 OPENVPN\_x\_DIGEST, 212  
 OPENVPN\_x\_DNSIP, 205  
 OPENVPN\_x\_DOMAIN, 205  
 OPENVPN\_x\_FLOAT, 213  
 OPENVPN\_x\_FRAGMENT, 216  
 OPENVPN\_x\_IPV6, 203  
 OPENVPN\_x\_ISDN\_CIRC\_NAME, 213  
 OPENVPN\_x\_KEYSIZ, 213  
 OPENVPN\_x\_LINK\_MTU, 216  
 OPENVPN\_x\_LOCAL\_HOST, 199  
 OPENVPN\_x\_LOCAL\_PORT, 199  
 OPENVPN\_x\_LOCAL\_VPN\_IP, 202  
 OPENVPN\_x\_LOCAL\_VPN\_IPV6, 203  
 OPENVPN\_x\_MANAGEMENT\_LOG\_-  
     CACHE, 213  
 OPENVPN\_x\_MSSFIX, 216  
 OPENVPN\_x\_MUTE\_REPLAY\_-  
     WARNINGS, 214  
 OPENVPN\_x\_NAME, 212  
 OPENVPN\_x\_OPEN\_OVPNPORT, 214  
 OPENVPN\_x\_PF6\_FORWARD\_N, 215  
 OPENVPN\_x\_PF6\_FORWARD\_x, 215  
 OPENVPN\_x\_PF6\_INPUT\_N, 215  
 OPENVPN\_x\_PF6\_INPUT\_x, 215  
 OPENVPN\_x\_PF\_DMZ\_TYPE, 441  
 OPENVPN\_x\_PF\_FORWARD\_LOG,  
     214  
 OPENVPN\_x\_PF\_FORWARD\_N, 215  
 OPENVPN\_x\_PF\_FORWARD\_-  
     POLICY, 215  
 OPENVPN\_x\_PF\_FORWARD\_x, 215  
 OPENVPN\_x\_PF\_INPUT\_LOG, 214  
 OPENVPN\_x\_PF\_INPUT\_N, 214  
 OPENVPN\_x\_PF\_INPUT\_POLICY,  
     214  
 OPENVPN\_x\_PF\_INPUT\_x, 214  
 OPENVPN\_x\_PF\_POSTROUTING\_N,  
     215  
 OPENVPN\_x\_PF\_POSTROUTING\_x,  
     215  
 OPENVPN\_x\_PF\_PREROUTING\_N,  
     215  
 OPENVPN\_x\_PF\_PREROUTING\_x,  
     215  
 OPENVPN\_x\_PING, 213  
 OPENVPN\_x\_PING\_RESTART, 213  
 OPENVPN\_x\_PROTOCOL, 213  
 OPENVPN\_x\_REMOTE\_HOST, 198

- OPENVPN\_x\_REMOTE\_HOST\_N, 198
- OPENVPN\_x\_REMOTE\_HOST\_x, 199
- OPENVPN\_x\_REMOTE\_PORT, 199
- OPENVPN\_x\_REMOTE\_VPN\_IP, 202
- OPENVPN\_x\_REMOTE\_VPN\_IPV6, 203
- OPENVPN\_x\_RESOLV\_RETRY, 213
- OPENVPN\_x\_RESTART, 214
- OPENVPN\_x\_ROUTE\_N, 203
- OPENVPN\_x\_ROUTE\_x, 204
- OPENVPN\_x\_ROUTE\_x\_DNSIP, 205
- OPENVPN\_x\_ROUTE\_x\_DOMAIN, 205
- OPENVPN\_x\_SECRET, 200
- OPENVPN\_x\_SHAPER, 216
- OPENVPN\_x\_START, 213
- OPENVPN\_x\_TUN\_MTU, 216
- OPENVPN\_x\_TUN\_MTU\_EXTRA, 216
- OPENVPN\_x\_TYPE, 200
- OPENVPN\_x\_VERBOSE, 213
- OPT\_ADDMODULES, 436
- OPT\_ARP, 443
- OPT\_ATH\_INFO, 273
- OPT\_AUTOMOUNT, 162
- OPT\_BCRELAY, 113, 443
- OPT\_BMON, 266
- OPT\_BONDING\_DEV, 114
- OPT\_BRIDGE\_DEV, 120
- OPT\_CERT, 128
- OPT\_CERT\_X509, 128
- OPT\_CHRONY, 130
- OPT\_CIRCUIT\_STATUS, 103
- OPT\_CURL, 266
- OPT\_DHCP, 138
- OPT\_DHCP\_CLIENT, 143
- OPT\_DHCPDUMP, 271
- OPT\_DHCPRELAY, 142
- OPT\_DIG, 267
- OPT\_DMZ, 434, 436
- OPT\_DNS, 132
- OPT\_DYNDNS, 154
- OPT\_E3, 273
- OPT\_EASYCRON, 156
- OPT\_EBTABLES, 123
- OPT\_ETHTOOL, 126, 443
- OPT\_EVSS, 434, 436
- OPT\_EXTMOUNT, 161
- OPT\_FASTD, 286
- OPT\_FLASHROM, 273
- OPT\_FTP, 267
- OPT\_HDDRV, 164
- OPT\_HDINSTALL, 158
- OPT\_HDINSTALL\_TEST, 439
- OPT\_HDSLEEP, 163
- OPT\_HOSTS, 131
- OPT\_HOTPLUG\_PCI, 110
- OPT\_HTTPD, 165
- OPT\_HW\_DETECT, 273
- OPT\_HWSUPP, 170
- OPT\_I2CTOOLS, 273
- OPT\_IFTOP, 267
- OPT\_IMONC, 267
- OPT\_IMOND, 83
- OPT\_IPERF, 267
- OPT\_IPV4, 41
- OPT\_IPV6, 45, 439
- OPT\_ISDN, 179
- OPT\_ISDN\_COMP, 183
- OPT\_IWLEEPROM, 273
- OPT\_KLOGD, 107, 436
- OPT\_LNSTAT, 268
- OPT\_LOGIP, 107, 436
- OPT\_LSPCI, 273
- OPT\_MAKEKBL, 38, 436
- OPT\_MOUNT, 160
- OPT\_MOUNTFLOPPY, 434, 436
- OPT\_MTOOLS, 274
- OPT\_MULTILINK\_PPP, 237
- OPT\_NET\_PREFIX, 46
- OPT\_NETCAT, 268
- OPT\_NETIO, 268
- OPT\_NETSTAT, 443
- OPT\_NGREP, 268
- OPT\_NMAP, 268
- OPT\_NTTCP, 268
- OPT\_OAC, 167
- OPT\_OPENSSL, 274
- OPT\_OPENVPN, 198
- OPT\_PCMCIA, 224
- OPT\_PLINK\_CLIENT, 266
- OPT\_PNP, 108, 436
- OPT\_PPP, 225
- OPT\_PPP\_DSLMODEM, 148
- OPT\_PPP\_ETHERNET, 242

- OPT\_PPP\_ETHERNET\_SERVER, 243
- OPT\_PPP\_PPTP, 280
- OPT\_PPP\_PPTP\_SERVER, 281
- OPT\_PPP\_SERIAL, 240
- OPT\_PPP\_SERIAL\_SERVER, 240
- OPT\_QOS, 246
- OPT\_RCAPID, 195
- OPT\_REAVER, 274
- OPT\_RECOVER, 164
- OPT\_RTMON, 270
- OPT\_SCP, 443
- OPT\_SERIAL, 443
- OPT\_SFTPSERVER, 266
- OPT\_SHRED, 274
- OPT\_SOCAT, 270
- OPT\_SSH\_CLIENT, 265
- OPT\_SSHD, 261
- OPT\_STRACE, 274
- OPT\_STUN, 156
- OPT\_SWITCH, 124
- OPT\_SYSLOGD, 105, 436
- OPT\_TCPDUMP, 270
- OPT\_TELMOND, 192
- OPT\_TFTP, 147
- OPT\_TRACEPATH, 270
- OPT\_TRACEROUTE, 443
- OPT\_TRACEROUTE6, 443
- OPT\_UMTS, 275
- OPT\_USB, 277
- OPT\_VALGRIND, 274
- OPT\_VLAN\_DEV, 118
- OPT\_VPN\_CARD, 175
- OPT\_WGET, 272
- OPT\_WLAN, 286
- OPT\_Y2K, 107, 436
- OPT\_YADIFA, 147
- OPT\_YADIFA\_SLAVE\_ZONE\_-  
USE\_DNSMASQ\_ZONE\_-  
DELEGATION, 148
- OPT\_YADIFA\_USE\_DNSMASQ\_-  
ZONE\_DELEGATION, 147
- OPT\_YTREE, 274
- PACKETFILTER\_LOG, 434, 436
- PACKETFILTER\_LOG\_LEVEL, 434,  
436
- PASSWORD, 28, 436
- PCMCIA\_CARDMGR\_OPTS, 441
- PCMCIA\_CORE\_OPTS, 441
- PCMCIA\_MISC\_N, 225
- PCMCIA\_MISC\_x, 225
- PCMCIA\_PCIC, 224
- PCMCIA\_PCIC\_EXTERN, 441
- PCMCIA\_PCIC\_OPTS, 225
- PF6\_FORWARD\_ACCEPT\_DEF, 78,  
439
- PF6\_FORWARD\_LOG, 79, 439
- PF6\_FORWARD\_LOG\_LIMIT, 79, 439
- PF6\_FORWARD\_N, 79, 439
- PF6\_FORWARD\_POLICY, 78, 439
- PF6\_FORWARD\_REJ\_LIMIT, 79, 440
- PF6\_FORWARD\_UDP\_REJ\_LIMIT,  
79, 440
- PF6\_FORWARD\_x, 79, 440
- PF6\_FORWARD\_x\_COMMENT, 80, 440
- PF6\_INPUT\_ACCEPT\_DEF, 77, 440
- PF6\_INPUT\_ICMP\_ECHO\_REQ\_-  
LIMIT, 77
- PF6\_INPUT\_ICMP\_ECHO\_REQ\_-  
SIZE, 78
- PF6\_INPUT\_LOG, 77, 440
- PF6\_INPUT\_LOG\_LIMIT, 77, 440
- PF6\_INPUT\_N, 78, 440
- PF6\_INPUT\_POLICY, 77, 440
- PF6\_INPUT\_REJ\_LIMIT, 77, 440
- PF6\_INPUT\_UDP\_REJ\_LIMIT, 77, 440
- PF6\_INPUT\_x, 78, 440
- PF6\_INPUT\_x\_COMMENT, 78, 440
- PF6\_LOG\_LEVEL, 76
- PF6\_OUTPUT\_ACCEPT\_DEF, 80
- PF6\_OUTPUT\_LOG, 80
- PF6\_OUTPUT\_LOG\_LIMIT, 80
- PF6\_OUTPUT\_N, 80
- PF6\_OUTPUT\_POLICY, 80
- PF6\_OUTPUT\_REJ\_LIMIT, 80
- PF6\_OUTPUT\_UDP\_REJ\_LIMIT, 80
- PF6\_OUTPUT\_x, 81
- PF6\_OUTPUT\_x\_COMMENT, 81
- PF6\_POSTROUTING\_N, 82
- PF6\_POSTROUTING\_x, 82
- PF6\_POSTROUTING\_x\_COMMENT,  
82
- PF6\_PREROUTING\_N, 82
- PF6\_PREROUTING\_x, 82

- PF6\_PREROUTING\_x\_COMMENT, 82
- PF6\_USR\_CHAIN\_N, 81, 440
- PF6\_USR\_CHAIN\_x\_NAME, 81, 440
- PF6\_USR\_CHAIN\_x\_RULE\_N, 81, 440
- PF6\_USR\_CHAIN\_x\_RULE\_x, 81, 440
- PF6\_USR\_CHAIN\_x\_RULE\_x\_-  
COMMENT, 82, 440
- PF\_FORWARD\_ACCEPT\_DEF, 62, 436
- PF\_FORWARD\_LOG, 62, 436
- PF\_FORWARD\_LOG\_LIMIT, 62, 436
- PF\_FORWARD\_N, 63, 434, 436
- PF\_FORWARD\_POLICY, 62, 436
- PF\_FORWARD\_REJ\_LIMIT, 62, 436
- PF\_FORWARD\_UDP\_REJ\_LIMIT, 62,  
436
- PF\_FORWARD\_x, 63, 436
- PF\_FORWARD\_x\_COMMENT, 63, 436
- PF\_INPUT\_ACCEPT\_DEF, 60, 436
- PF\_INPUT\_ICMP\_ECHO\_REQ\_-  
LIMIT, 61, 436
- PF\_INPUT\_ICMP\_ECHO\_REQ\_SIZE,  
61
- PF\_INPUT\_LOG, 61, 436
- PF\_INPUT\_LOG\_LIMIT, 61, 436
- PF\_INPUT\_N, 61, 434, 436
- PF\_INPUT\_POLICY, 60, 436
- PF\_INPUT\_REJ\_LIMIT, 61, 436
- PF\_INPUT\_UDP\_REJ\_LIMIT, 61, 436
- PF\_INPUT\_x, 61, 436
- PF\_INPUT\_x\_COMMENT, 61, 436
- PF\_LOG\_LEVEL, 60, 436
- PF\_NEW\_CONFIG, 49, 434, 436
- PF\_OUTPUT\_ACCEPT\_DEF, 63
- PF\_OUTPUT\_CT\_ACCEPT\_DEF, 76
- PF\_OUTPUT\_CT\_N, 76
- PF\_OUTPUT\_CT\_x, 76
- PF\_OUTPUT\_CT\_x\_COMMENT, 76
- PF\_OUTPUT\_LOG, 63
- PF\_OUTPUT\_LOG\_LIMIT, 63
- PF\_OUTPUT\_N, 64
- PF\_OUTPUT\_POLICY, 63
- PF\_OUTPUT\_REJ\_LIMIT, 64
- PF\_OUTPUT\_UDP\_REJ\_LIMIT, 64
- PF\_OUTPUT\_x, 64
- PF\_OUTPUT\_x\_COMMENT, 64
- PF\_POSTROUTING\_N, 65, 434, 436
- PF\_POSTROUTING\_x, 65, 436
- PF\_POSTROUTING\_x\_COMMENT,  
65, 436
- PF\_PREROUTING\_CT\_ACCEPT\_-  
DEF, 76
- PF\_PREROUTING\_CT\_N, 76
- PF\_PREROUTING\_CT\_x, 76
- PF\_PREROUTING\_CT\_x\_-  
COMMENT, 76
- PF\_PREROUTING\_N, 66, 434, 436
- PF\_PREROUTING\_x, 66, 436
- PF\_PREROUTING\_x\_COMMENT, 66,  
436
- PF\_USR\_CHAIN\_N, 64, 434, 436
- PF\_USR\_CHAIN\_x\_NAME, 64, 436
- PF\_USR\_CHAIN\_x\_RULE\_N, 64, 434,  
436
- PF\_USR\_CHAIN\_x\_RULE\_x, 64, 436
- PF\_USR\_CHAIN\_x\_RULE\_x\_-  
COMMENT, 64, 436
- PORTFW\_N, 434, 436
- PORTFW\_x\_COMMENT, 436
- PORTFW\_x\_NEW\_TARGET, 436
- PORTFW\_x\_PROTOCOL, 437
- PORTFW\_x\_TARGET, 437
- POWERMANAGEMENT, 33, 437
- PPP\_COMP\_LZSCOMP\_LEVEL, 234
- PPP\_DEV, 441
- PPP\_IPADDR, 441
- PPP\_NETMASK, 441
- PPP\_NETWORK, 441
- PPP\_PEER, 441
- PPP\_SPEED, 441
- pptp, 76
- PRESERVE, 434, 437
- PXESUBDIR, 314
- QOS\_CLASS\_N, 247
- QOS\_CLASS\_x\_DIRECTION, 248
- QOS\_CLASS\_x\_LABEL, 249
- QOS\_CLASS\_x\_MAXBANDWIDTH,  
248
- QOS\_CLASS\_x\_MINBANDWIDTH, 247
- QOS\_CLASS\_x\_PARENT, 247
- QOS\_CLASS\_x\_PRIO, 249
- QOS\_FILTER\_N, 249
- QOS\_FILTER\_x\_CLASS, 250
- QOS\_FILTER\_x\_IP\_EXTERN, 251

- QOS\_FILTER\_x\_IP\_INTERN, 250
- QOS\_FILTER\_x\_OPTION, 252
- QOS\_FILTER\_x\_PORT, 251
- QOS\_FILTER\_x\_PORT\_TYPE, 251
- QOS\_INTERNET\_BAND\_DOWN, 246
- QOS\_INTERNET\_BAND\_UP, 246
- QOS\_INTERNET\_DEFAULT\_DOWN, 246
- QOS\_INTERNET\_DEFAULT\_UP, 247
- QOS\_INTERNET\_DEV\_N, 246
- QOS\_INTERNET\_DEV\_x, 246
  
- RCAPID\_PORT, 195
- REMOTEHOSTNAME, 313
- REMOTEPATHNAME, 313
- REMOTEPORT, 314
- REMOTEREMOUNT, 314
- REMOTEUPDATE, 313
- REMOTEUSERNAME, 313
- ROUTE\_NETWORK, 434, 437
- RTC\_SYNC, 31
  
- sane, 76
- SER\_CONSOLE, 35, 437
- SER\_CONSOLE\_IF, 36, 437
- SER\_CONSOLE\_RATE, 36, 437
- sip, 76
- snmp, 76
- SQUEEZE\_SCRIPTS, 314
- SSH\_CLIENT\_PRIVATE\_KEYFILE\_N, 265
- SSH\_CLIENT\_PRIVATE\_KEYFILE\_x, 265
- SSHD\_ALLOWPASSWORDLOGIN, 261
- SSHD\_CREATEHOSTKEYS, 261
- SSHD\_PORT, 263
- SSHD\_PUBLIC\_KEY\_N, 263
- SSHD\_PUBLIC\_KEY\_x, 264
- SSHD\_PUBLIC\_KEYFILE\_N, 264
- SSHD\_PUBLIC\_KEYFILE\_x, 264
- SSHKEYFILE, 314
- START\_IMOND, 434, 437
- STUN\_SERVER\_N, 156
- STUN\_SERVER\_x, 156
- SWITCH\_N, 124
- SWITCH\_x\_DEV, 124
- SWITCH\_x\_VLAN\_N, 124
- SWITCH\_x\_VLAN\_y\_ID, 124
- SWITCH\_x\_VLAN\_y\_PORT\_N, 124
- SWITCH\_x\_VLAN\_y\_PORT\_z\_ID, 124
- SWITCH\_x\_VLAN\_y\_PORT\_z\_MODE, 124
- SYSLOGD\_DEST\_N, 105, 434, 437
- SYSLOGD\_DEST\_x, 105, 437
- SYSLOGD\_RECEIVER, 105, 437
- SYSLOGD\_ROTATE, 106, 437
- SYSLOGD\_ROTATE\_AT\_SHUTDOWN, 107
- SYSLOGD\_ROTATE\_DIR, 107, 437
- SYSLOGD\_ROTATE\_MAX, 107, 437
  
- TELMOND\_CAPI\_CTRL\_N, 194
- TELMOND\_CAPI\_CTRL\_x, 195
- TELMOND\_CMD\_N, 194
- TELMOND\_CMD\_x, 194
- TELMOND\_LOG, 193
- TELMOND\_LOGDIR, 193
- TELMOND\_MSN\_N, 193
- TELMOND\_MSN\_x, 193
- TELMOND\_PORT, 193
- tftp, 76
- TFTP\_PATH, 147
- TFTPBOOTIMAGE, 314
- TFTPBOOTPATH, 314
- TIME\_INFO, 30, 437
- TRUSTED\_NETS, 434, 437
  
- UCLIBC\_COMPAT, 444
- UMTS\_ADAPTER, 275
- UMTS\_APN, 443
- UMTS\_CHARGEINT, 443
- UMTS\_CTRL, 276
- UMTS\_DEBUG, 275
- UMTS\_DEV, 276
- UMTS\_DIALOUT, 443
- UMTS\_DRV, 276
- UMTS\_FILTER, 443
- UMTS\_GPRS\_UMTS, 275
- UMTS\_HUP\_TIMEOUT, 444
- UMTS\_IDDEVICE, 276
- UMTS\_IDDEVICE2, 276
- UMTS\_IDVENDOR, 275
- UMTS\_IDVENDOR2, 276



UMTS\_NAME, [444](#)  
 UMTS\_PASSWD, [444](#)  
 UMTS\_PIN, [275](#)  
 UMTS\_SWITCH, [276](#)  
 UMTS\_TIMES, [444](#)  
 UMTS\_USEPEERDNS, [444](#)  
 UMTS\_USER, [444](#)  
 USB\_EXTRA\_DRIVER\_N, [277](#)  
 USB\_EXTRA\_DRIVER\_x, [277](#)  
 USB\_EXTRA\_DRIVER\_x\_PARAM, [278](#)  
 USB\_LOWLEVEL, [444](#)  
 USB\_MODEM\_WAITSECONDS, [278](#)  
  
 VERBOSE, [313](#)  
 VLAN\_DEV\_N, [118](#)  
 VLAN\_DEV\_x\_DEV, [118](#)  
 VLAN\_DEV\_x\_VID, [118](#)  
 VPN\_CARD\_TYPE, [175](#)  
  
 WGET\_SSL, [443](#)  
 WLAN\_N, [287](#)  
 WLAN\_REGDOMAIN, [286](#)  
 WLAN\_x\_ACL\_MAC\_N, [290](#)  
 WLAN\_x\_ACL\_MAC\_x, [290](#)  
 WLAN\_x\_ACL\_POLICY, [290](#)  
 WLAN\_x\_AP, [289](#)  
 WLAN\_x\_BRIDGE, [291](#)  
 WLAN\_x\_CHANNEL, [287](#)  
 WLAN\_x\_DIVERSITY, [290](#)  
 WLAN\_x\_DIVERSITY\_RX, [290](#)  
 WLAN\_x\_DIVERSITY\_TX, [290](#)  
 WLAN\_x\_ENC\_ACTIVE, [288](#)  
 WLAN\_x\_ENC\_MODE, [289](#)  
 WLAN\_x\_ENC\_N, [288](#)  
 WLAN\_x\_ENC\_x, [288](#)  
 WLAN\_x\_ESSID, [287](#)  
 WLAN\_x\_MAC, [287](#)  
 WLAN\_x\_MAC\_OVERRIDE, [287](#)  
 WLAN\_x\_MODE, [287](#)  
 WLAN\_x\_NOESSID, [287](#)  
 WLAN\_x\_PSKFILE, [290](#)  
 WLAN\_x\_RATE, [288](#)  
 WLAN\_x\_RTS, [288](#)  
 WLAN\_x\_WPA\_DEBUG, [289](#)  
 WLAN\_x\_WPA\_ENCRYPTION, [289](#)  
 WLAN\_x\_WPA\_KEY\_MGMT, [289](#)  
  
 WLAN\_x\_WPA\_PSK, [289](#)  
 WLAN\_x\_WPA\_TYPE, [289](#)  
 WLAN\_x\_WPS, [290](#)  
  
 Y2K\_DAYS, [108](#), [437](#)  
 YADIFA\_ALLOW\_QUERY\_N, [147](#)  
 YADIFA\_ALLOW\_QUERY\_x, [147](#)  
 YADIFA\_LISTEN\_N, [147](#)  
 YADIFA\_SLAVE\_ZONE\_N, [148](#)  
 YADIFA\_SLAVE\_ZONE\_x, [148](#)  
 YADIFA\_SLAVE\_ZONE\_x\_ALLOW\_-  
     QUERY\_N, [148](#)  
 YADIFA\_SLAVE\_ZONE\_x\_ALLOW\_-  
     QUERY\_x, [148](#)  
 YADIFA\_SLAVE\_ZONE\_x\_MASTER,  
     [148](#)