

# **Paket C3SURF - Zugangskontrolle Version 2.3.1**

## **für den fli4l Version 3.10.3**

Frank Saurbier

E-Mail: [c3surf@arcor.de](mailto:c3surf@arcor.de)

TexSatz: Helmut Backhaus

E-Mail: [helmut.backhaus@gmx.de](mailto:helmut.backhaus@gmx.de)

Das fli4l-Team

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

26. Juli 2015

# Inhaltsverzeichnis

<b>1. Dokumentation des Paketes C3SURF</b>	<b>3</b>
1.1. Einleitung . . . . .	3
1.2. Hinweise zur Installation . . . . .	3
1.3. Konfiguration OPT_C3SURF . . . . .	3
1.3.1. Optionale Parameter OPT_C3SURF . . . . .	11
1.4. Dokumentation der Funktion LOGINUSR für C3SURF . . . . .	12
1.5. Konfiguration OPT_LOGINUSER für C3SURF . . . . .	13
1.5.1. Optionale Parameter OPT_LOGINUSR . . . . .	14
1.6. Dokumentation der Funktion VOUCHER für C3SURF . . . . .	15
1.7. Konfiguration von OPT_VOUCHER . . . . .	15
1.7.1. Optionale Parameter OPT_VOUCHER . . . . .	16
1.8. Dokumentation der Funktion Traffic für C3SURF . . . . .	18
1.9. Konfiguration OPT_C3SURF_TRAFFIC . . . . .	19
1.10. Allgemeines zu C3SURF . . . . .	20
1.11. fli4l Webinterface . . . . .	20
1.12. Funktionsweise . . . . .	20
1.13. Namensauflösung - DNS . . . . .	22
1.14. Sonstiges zu C3SURF . . . . .	22
1.14.1. Warnung . . . . .	22
1.14.2. Empfehlung . . . . .	22
1.14.3. Fehler . . . . .	22
1.14.4. Lizenz . . . . .	23
1.14.5. Literatur . . . . .	23
<b>A. Anhang zum Paket C3SURF</b>	<b>24</b>
A.1. Tips zu anderen Opts . . . . .	24
A.1.1. cpmvrmllog Config . . . . .	24
A.1.2. Samba ohne Anmeldung erlauben . . . . .	24
A.1.3. Migration aus Vorgängerversionen . . . . .	25
<b>Index</b>	<b>27</b>

# 1. Dokumentation des Paketes C3SURF

## 1.1. Einleitung

Mit C3SURF kann man ein offenes, nicht verschlüsseltes Netz/WLAN betreiben. Schon aus rechtlichen Gründen sollte man jedoch kontrollieren, wer das Netz nutzt. C3SURF ermöglicht eine formlose Registrierung im Netz. Das Paket basiert auf “opt\_onco” (Copyright (c) 2001-2007 Michael Mattes). Durch die Nutzung von OPT\_LOGINUSR kann eine “fast” echte Anmeldung nachgestellt werden. C3SURF kann auch Gutscheine generieren und eine rudimentäre (experimentelle) Steuerungsfunktion zur Unterbindung von übermäßigem Download-Volumen ist ebenfalls integriert.

Man definiert, welche Hosts oder kompletten Netze von C3SURF verwaltet werden. Diese sind nach einem Routerstart zunächst gesperrt und deren http Anfragen werden auf die C3SURF Anmeldeseite geleitet. Nach der Registrierung eines Benutzers auf der Anmeldeseite wird eine Nutzung auf Zeit erlaubt. Alles wird protokolliert und über das Webinterface von C3SURF gesteuert.

## 1.2. Hinweise zur Installation

- Wie immer bei Opt-Paketen für den fli4l:
  - opt\_c3surf\_<versionsinfo>.tar.gz in das fli4l Verzeichnis (Buildrechner) entpacken.
  - c3surf.txt den eigenen Bedürfnissen anpassen.
  - ggf. in der httpd.txt die Rechte 'c3surf:view,admin' hinzufügen.
  - Build erstellen.

**Wichtig:** Der fli4l muss als DNS-Server bei den Clients eingetragen sein und muss befähigt sein Namen aufzulösen. Dazu

- benötigt er einen “Forward” auf den DNS-Server des Netzes oder
- er ist selbst der DNS-Server und kann ggf. automatisch Verbindungen aufbauen.

Sonst gibt es Probleme auf die Anmeldeseite umzuleiten. Diese kann aber immer noch manuell durch die Eingabe ihrer URL aufgerufen werden.

## 1.3. Konfiguration OPT\_C3SURF

**OPT\_C3SURF** Standard-Einstellung: OPT\_C3SURF='no'

Paket aktivieren oder deaktivieren.

**C3SURF\_LOG\_PATH** Standard-Einstellung: `C3SURF_LOG_PATH='/var/log/c3surf'`

Definiert das Verzeichnis für log-Dateien von C3SURF. Beim Herunterfahren sollten die Logdateien auf ein permanentes Medium gesichert oder gleich der Pfad dorthin eingestellt werden, wenn man die Dateien behalten will. Der Pfad muss auf dem permanenten Medium existieren.

**Wichtig:** Die `'c3surf_mac.blacklist'` liegt im persistenten Verzeichnis [C3SURF\\_PERSISTENT\\_PATH](#) (Seite 4). Eine eigene Blacklist muss dorthin kopiert werden. Der Umfang des Protokolls wird im Folgenden definiert.

**C3SURF\_DOLOG\_LOGIN** Standard-Einstellung: `C3SURF_DOLOG_LOGIN='yes'`

Zeichne Login/Logout auf: `c3surf_login.log` (default: 'yes')

**C3SURF\_DOLOG\_INVALID** Standard-Einstellung: `C3SURF_DOLOG_INVALID='yes'`

Zeichne ungültige Logins auf: `c3surf_invalid.log` (default: 'yes'). Wenn [OPT\\_LOGINUSR](#) (Seite 13) = 'yes' gesetzt ist, kann eine fehlerhafte Anmeldung nicht aufgezeichnet werden.

**C3SURF\_DOLOG\_PAGE** Standard-Einstellung: `C3SURF_DOLOG_PAGE='no'`

Zeichne den Aufruf der html-Seite auf: `c3surf_page.log` (default: 'no'). Jeder Zugriff auf die Anmeldeseite wird gelogged. Das Page-Log wächst schnell und ist daher nur für "Neugierige" empfohlen.

**C3SURF\_DOLOG\_HTTPD** Standard-Einstellung: `C3SURF_DOLOG_HTTPD='no'`

Zeichne alle mini\_httpd Anfragen auf: `c3surf_httpd.log` (default: 'no').

**Wichtig:** Zusätzlich die Mini-httpd Logfunktion starten (bitte nur für Test oder Debuggingzwecke verwenden). Wenn eingeschaltet, empfiehlt es sich regelmäßig das Protokoll zu prüfen und zu löschen, das es sehr schnell groß wird.

`opt_cpmvrmlog`: [http://extern.fli4l.de/fli4l\\_opt-db3/search.pl?pid=427](http://extern.fli4l.de/fli4l_opt-db3/search.pl?pid=427) kann zum regelmäßigen Sichern benutzt werden. Damit danach wieder korrekt gelogged wird, muss der mini\_httpd neu gestartet werden.

Dazu gibt es das Script `/usr/local/bin/c3surf_kill_httpd.sh` ([Config Beispiel im Anhang](#)). (Seite 24)

**C3SURF\_PERSISTENT\_PATH** Unbedingt anpassen, Empfehlung: `'/var/lib/persistent/c3surf'`

Definiert das Verzeichnis für Dateien, die nach dem Ausschalten oder nach einem Reboot erhalten bleiben sollen. Idealerweise liegt dies auf einer Festplatte oder CF-Karte (`'/var/lib/persistent/c3surf'`). Es kann auch ein Verzeichnis in der RAM-Disk gewählt werden (z.B. um das Medium zu schonen). Dann sollte das Verzeichnis sporadisch auf die Platte kopiert werden (z.B. `opt_cpmvrmlog`), da die Daten sonst nach einem Reboot, Absturz oder Stromverlust verloren wären.

**Was wird hier gespeichert:**

### MAC-Blackliste:

'c3surf\_mac.blacklist', wird bei Bedarf angelegt (siehe Admin Interface). Die Sperrung für die Mac-Adresse wurde über eine eigene Datei und nicht über den Paketfilter gelöst, da eine größeren Zahl von Einträgen Probleme auslösen kann. Nicht vergessen: Geblockte MAC-Adressen halten Standardbenutzer vom Netz fern, was im normalen Anwendungsfall ausreicht, nicht jedoch die Profis. Diese MAC-Blacklist verhindert nur die Anmeldung über C3SURF / loginusr, weil nichts direkt in der Firewall gesperrt wird.

### Benutzerdaten:

<userloginname>.data (z. B. 'frank.data'), diese Dateien enthalten Daten über die Benutzer, wie Vorname, Name und E-mail-Adresse, Statistiken und Quotas. Die Persistenz der Benutzerdaten ermöglicht, dass die Daten aus der Konfigurationsdatei nur beim ersten Mal erzeugt werden. Das heißt: Ist für den Benutzer "frank" eine 'frank.data' beim Systemstart vorhanden, so werden die Einstellungen in der Config-Datei ignoriert.

Mittels `LOGINUSR_ACCOUNT_x_OVERWRITE='yes'` (Seite 14) kann das überschreiben der entsprechenden Benutzerdaten erzwungen werden.

Mittels `LOGINUSR_DELETE_PERSISTENT_DATA='yes'` (Seite 13), werden alle "\*.data" Dateien beim Reboot gelöscht.

**C3SURF\_WORKON\_TMP** Standard-Einstellung: `C3SURF_WORKON_TMP='no'`

Wer `C3SURF_PERSISTENT_PATH` (Seite 4) eingestellt hat, kann hier 'yes' eintragen. Persistenten Daten werden dann beim Systemstart von der Festplatte auf das Verzeichnis `C3SURF_TMP_PATH` kopiert und nur noch von dort gelesen. Auf die Festplatte wird dann von C3SURF nur noch zugegriffen, wenn durch den Admin Daten in die persistenten Dateien geschrieben werden.

**Wichtig:** *Persistente Daten sind:*

- Benutzer-Accounts
- MAC-Blackliste
- System Lock Datei (Verhindern jeder Anmeldung)

*Für FLASH-Speicher kann hier 'no' stehen, da ja im normalen Betrieb von C3SURF nur gelesen wird. Schreibzugriffe verursacht nur der Admin.*

**C3SURF\_QUOTA** Standard-Einstellung: `C3SURF_QUOTA='no'`

Soll der Zugang limitiert werden, wird hier 'yes' eingetragen. So wird der Zugang für eine IP-Adresse für `C3SURF_BLOCKTIME` (Seite 7) Minuten nach Zeitablauf oder

Überschreitung des Anmeldezählers blockiert. Standardwert ist 'yes'.

**Wichtig:** Auch die individuellen *-TIME*, *-BLOCKTIME* und *-COUNTER* bei den Accounts zum *LOGIN\_USR* werden durch diese Variable aktiviert ('yes') oder deaktiviert ('no').

**C3SURF\_COUNTER** Standard-Einstellung: C3SURF\_COUNTER='0'

Gibt die Anzahl der möglichen Unterbrechungen innerhalb der Freiminuten an.

**Wichtig:** Es kann eine Anzahl von Unterbrechungen (Logout/Login) definiert werden. Wird hier z. B. '1' eingetragen, so kann man sich innerhalb der Freiminuten einmal abmelden und dann wieder anmelden, was 2 Anmeldungen in der Zeit entspricht. Bei der folgenden Anmeldung erhält man die von *C3SURF\_TIME* (Seite 7) noch verbliebene Differenz von der Anmeldung davor.

Ist zudem *C3SURF\_BLOCKTIME='0'* (Seite 7) gesetzt wird der *C3SURF\_COUNTER* (Seite 6) erst nach 0:00 Uhr des Folgetages zurückgesetzt.

- Mit C3SURF\_COUNTER='0'

entspricht der Wert dem Parkuhrprinzip (Geld rein, Geld weg, Zeit läuft: also keine Unterbrechungen möglich).

- Mit C3SURF\_COUNTER='1'

wird diese Funktion abgeschaltet = beliebig viele Unterbrechungen der Freiminuten sind möglich.

- Mit C3SURF\_COUNTER='2'

gibt es beliebig viele Unterbrechungen (wie '1'), aber die Blockzeit wird bereits mit der ersten Anmeldung heruntergezählt. Im Gegensatz zur '1', wo die Blockzeit erst nach dem Verbrauch der gesamten Zeit eingestellt wird. Da hier die Blockzeit gleichzeitig heruntergezählt wird, wird der Benutzer nur geblockt, wenn er sein Kontingent zu schnell verbraucht.

Erläuterungen zum Langzeitkontingent (C3SURF\_COUNTER='2'):

Damit kann man z. B. 10 Stunden Onlinezeit (*C3SURF\_TIME='600'*) (Seite 7) mit einer Blockzeit von einer Woche (*C3SURF\_BLOCKTIME='10080'*) (Seite 7) : 60sec x 24h x 7Tage) kombinieren. Dann können die 10 Stunden innerhalb einer Woche verbraucht werden. Wer sie am ersten Tag am Stück verbraucht, der wartet dann eben den Rest der Woche. Nach Ablauf der Blockzeit werden wieder 10 Stunden bereitgestellt.

Kurzfassung: Der Nutzer hat ein Wochenkontingent von 10 Stunden, welches er sich selbst sinnvoll auf die Woche verteilen kann. Verbraucht er das Kontingent nicht innerhalb einer Woche, dann wird er nicht mit einem "Quota-Block" belegt. Es entsteht dann keine Wartezeit. Verbraucht er es hingegen am ersten Tag, dann ist

er die restlichen 6 Tage der Woche geblockt.

Gilt auch für `LOGINUSR_ACCOUNT_x_COUNTER` (Seite 14).

Empfehlung: `C3SURF_SAVE_QUOTA='yes'` (Seite 7), dann bleiben die Werte auch nach einem normalen Neustart erhalten.

Bei Stromausfall gehen die Werte verloren.

Ist `C3SURF_QUOTA='yes'` (Seite 5), so wird nach der Überschreitung des Zählers die Sperre entsprechend `C3SURF_BLOCKTIME` (Seite 7) aktiviert.

**C3SURF\_TIME** Standard-Einstellung: `C3SURF_TIME='60'`

Anzahl der Minuten, die eine Freischaltung gilt.

Wobei der Wert '0' ein unlimitiertes Login bedeutet (gilt auch für `LOGINUSR_ACCOUNT_x_TIME`).

Sonderfall:

- `C3SURF_TIME='0'`

Bedeutet eine unlimitierte Onlinezeit. Der Nutzer sollte sich selbst abmelden. Das System (C3SURF) meldet ihn nur ab, wenn der Rechner abgeschaltet wird und `C3SURF_CHECK_ARP='yes'` (Seite 8) (Standardeinstellung) gewählt wurde.

**C3SURF\_BLOCKTIME** Standard-Einstellung: `C3SURF_BLOCKTIME='240'`

Anzahl der Minuten, die eine IP geblockt wird, wenn die Freiminuten abgelaufen sind oder wenn der Admin dies über das Web-Interface veranlasst. So kann ein Rechner für diese Zeit aus dem Netz ferngehalten und die Nutzung eingeschränkt werden. Damit bei Zeitablauf die Sperrung erfolgt, muss `C3SURF_QUOTA='yes'` (Seite 5) eingestellt sein.

Sonderfälle:

- `C3SURF_BLOCKTIME='0'`

es erfolgt eine Sperrung der Adresse, bzw. des Nutzers bis 00:00 Uhr des Folgetages.

- `C3SURF_BLOCKTIME='-1'`

es erfolgt keine Sperrung.

**Wichtig:** Die Aufhebung der Sperre ist mit einem mittleren Fehler von einer Minute behaftet.

**C3SURF\_SAVE\_QUOTA** Standard-Einstellung: C3SURF\_SAVE\_QUOTA='yes'

Sichert die Quota-Werte beim Herunterfahren und lädt sie beim Start des Routers. Damit werden bei einem normalen Reboot des Routers die temporären Dateien der Quota-Verwaltung nach [C3SURF\\_PERSISTENT\\_PATH](#) (Seite 4) geschrieben und beim Neustart von dort wieder in das temporäre Verzeichnis kopiert. So bleiben die momentanen Verbrauchsdaten der Benutzer erhalten. Ein plötzlicher Ausfall ist damit nicht abgedeckt.

**Wichtig:** [LOGINUSR\\_DELETE\\_PERSISTENT\\_DATA='no'](#) (Seite 13), sollte eingestellt sein, weil diese Option sonst beim Neustart alle Benutzer-Accounts und die zugehörigen Quota-Daten löscht.

**C3SURF\_CHECK\_ARP** Standard-Einstellung: C3SURF\_CHECK\_ARP='yes'

Prüfe im Countdown Modul, ob die IP eines Rechners aus der ARP Tabelle verschwunden ist. So kann ein abgeschalteter Rechner erkannt werden, jedoch manchmal mit erheblichem Zeitversatz.

**C3SURF\_CONTROL\_HOST\_OR\_NET\_N** C3SURF\_CONTROL\_HOST\_OR\_NET\_N='0'

Wert: Ganze Zahl.

Wieviele und welche IP-Bereiche oder Hosts sollen von c3Surf kontrolliert werden? Dies betrifft die Weiterleitung in ein anderes Netz (FORWARD Chain).

**C3SURF\_CONTROL\_HOST\_OR\_NET\_x**

C3SURF\_CONTROL\_HOST\_OR\_NET\_x='Netzwerk OR Host OR IP-Adresse'

Kontrolliert alle Clients.

**Wichtig:** Hier kann zur Vereinfachung ein komplettes Netz angegeben werden, z.B. das WLAN. Dann müssen alle WLAN-Nutzer die Anmeldeseite benutzen. Es können auch eine Referenz auf einen Host (@Host) oder eine IP-Adresse angegeben werden. Wer oder was hier eingetragen ist, wird auf die Anmeldeseite umgeleitet und es gelten die weiter unten zu definierenden Sperrregeln.

Beispiel:

```
C3SURF_CONTROL_HOST_OR_NET_1='IP_NET_3'      # Das Netz angeben IP/MASK
C3SURF_CONTROL_HOST_OR_NET_2='@T8200'        # oder den Host @HOST
C3SURF_CONTROL_HOST_OR_NET_3='192.168.13.11'  # oder eine IP-Adresse
```

Das nächsten Beispiel ist vom Prinzip her gleich mit dem oben bereits dargestellten (IP\_NET\_3). Wenn in der "base.txt" die IP-Adresse so gesetzt wurde.

```
C3SURF_CONTROL_HOST_OR_NET_1='192.168.0.1/24' # kontrolliert alle Clients
```



## 1. Dokumentation des Paketes C3SURF

Soll ein Rechner ausgenommen sein, kann man entweder alle IP-Adressen einzeln in die C3SURF.txt aufnehmen (also eine Liste aller 256 Adressen erstellen, wobei man die eine weglässt), oder man verwendet die CIDR Notation (wie oben), dann sind es IP-Gruppen und damit weniger Schreibarbeit (8 Zeilen, statt 255).

Das sieht dann so aus:

```
C3SURF_CONTROL_HOST_OR_NET_N='8'           # Die Anzahl der Hosts
# oder Netze
C3SURF_CONTROL_HOST_OR_NET_1='192.168.0.0/31' # 0-1
C3SURF_CONTROL_HOST_OR_NET_2='192.168.0.3'   # only 3 not 2
C3SURF_CONTROL_HOST_OR_NET_3='192.168.0.4/30' # 4-7
C3SURF_CONTROL_HOST_OR_NET_4='192.168.0.8/29' # 8-15
C3SURF_CONTROL_HOST_OR_NET_5='192.168.0.16/28' # 16-31
C3SURF_CONTROL_HOST_OR_NET_6='192.168.0.32/27' # 32-63
C3SURF_CONTROL_HOST_OR_NET_7='192.168.0.64/26' # 64-127
C3SURF_CONTROL_HOST_OR_NET_8='192.168.0.128/25' # 128-255
```

Der Rechner mit der IP '192.168.0.2' kann ohne Anmeldung alles, was in der firewall des fli4l erlaubt ist.

**C3SURF\_CONTROL\_PORT\_N** C3SURF\_CONTROL\_PORT\_N='0'

Wert: Ganze Zahl.

Wieviele TCP-Ports des Routers sollen gesteuert werden?

Wieviele und welche explizit benannten Ports sollen von c3Surf kontrolliert werden? Betroffen sind die IP-Bereiche und die Hosts von oben

"C3SURF\_CONTROL\_HOST\_OR\_NET\_N" (Seite 8). c3Surf steuert diese Ports und gibt diese nach einer erfolgreichen Anmeldung frei, so dass die über diese Ports existierenden Services des Routers genutzt werden können (betrifft die INPUT-Chain).

**C3SURF\_CONTROL\_PORT\_x** C3SURF\_CONTROL\_PORT\_x='port\_nr'

Angabe der Portnummer und der Zugriff auf die dahinter stehenden Dienste des Routers (fli4l) sind bis zur Anmeldung gesperrt. Nach erfolgter Anmeldung wird der Dienst dann für die Zeit der Freischaltung zur Verfügung gestellt.

Beispiele:

```
C3SURF_CONTROL_PORT_1='515' # z.B. lpdsvr (Drucker benutzbar, nach Anmeldung)
C3SURF_CONTROL_PORT_2='21'  # z.B. ftp - (wohl gemerkt ftp auf dem router!)
```

Weitere mögliche Portadressen:

```
21=ftp
22=ssh
5000=imonc
5001=telmod
8118=privoxy
9050=tor
```

```
3128=squid
20000=mtgcapri
80=http(Admin)
515=lpdsrv
```

Entscheidend ist die eigene Konfiguration. Es gelten für alle Ports, die nicht angegeben sind immer die Regeln aus der 'base.txt'. Nach einer Anmeldung gelten immer noch die Regeln aus der 'base.txt'. c3Surf ist diesen Regeln bis zur Anmeldung durch den Benutzer nur vorgeschaltet. Es werden also nach der Anmeldung immer noch alle Regeln beachtet. So kann man z. B. in der 'base.txt' den Zugriff von WLAN auf das kabelgebundene Netz verbieten. Dieses Verbot gilt dann auch für die über c3Surf im WLAN angemeldeten Benutzer.

**C3SURF\_BLOCK\_PORT\_N** C3SURF\_BLOCK\_PORT\_N='0'

Wert: Ganze Zahl.

Wieviele TCP-Ports des Routers sollen geblockt werden?

Hinweise:

Permanentes Blocken von Diensten für oben benannte Netze und Hosts

"C3SURF\_CONTROL\_HOST\_OR\_NET\_N" (Seite 8). Wieviele und welche explizit benannten Ports sollen von c3Surf permanent geblockt werden? Es gibt dann keinen Zugriff auf die dahinter stehenden Dienste des Routers (fi4l) für die Hosts und/oder Rechner der gesperrten Netze, auch nach dem Anmelden nicht. Dies betrifft die INPUT-Chain. Wer bestimmte Dienste dauerhaft sperren will, sollte dies allerdings besser in der 'base.txt' mit den Parametern zur INPUT Chain tun.

Warum:

Weil diese Regeln hier nicht mehr gelten, sobald man den Parameter

OPT\_C3SURF='no' (Seite 3) setzt. Wer also C3SURF deaktiviert, muss zuvor die hier definierten Regeln in die 'base.txt' übertragen, wenn ihm die Sperre für die oben benannten Hosts oder Netze weiter wichtig sind.

**C3SURF\_BLOCK\_PORT\_x** C3SURF\_BLOCK\_PORT\_x='port\_nr'

Beispiele:

C3SURF_BLOCK_PORT_1='5000'	# z.B. imonc
C3SURF_BLOCK_PORT_2='5001'	# z.B. telmond
C3SURF_BLOCK_PORT_3='20000'	# z.B. mtgcapri (OPT_MTGCAPRI)
C3SURF_BLOCK_PORT_4='22'	# z.B. ssh
C3SURF_BLOCK_PORT_5='8118'	# z.B. privoxy (PROXY)
C3SURF_BLOCK_PORT_6='9050'	# z.B. tor (PROXY)
C3SURF_BLOCK_PORT_7='80'	# z.B. httpd Admin interface (HTTPD)
C3SURF_BLOCK_PORT_8='7437'	# z.B. caiviar (OPT_CAIVIAR)

**C3SURF\_HTTPD\_PORT** Standard-Einstellung: C3SURF\_HTTPD\_PORT='8080'

Auf welchem Port und welcher IP-Adresse soll der mini\_httpd für die Benutzeran-

meldung lauschen? http Anfragen von Rechnern werden auf diese Adresse und diesen Port umgeleitet. Port 8080 ist hier Default.

### Folgendes ist bei der Wahl der Portnummer zu beachten:

- Es sollte nicht der Port aus dem httpd-Paket sein (normal ist das 80).
- Der httpd für den Web-Admin des fli4l bindet sich im Standard an alle lokalen IP's.
- auch keine Portnummer benutzen, die bereits von einem anderen Dienst genutzt wird.

Sollte hier versehentlich ein bereits verwendeten Port definiert sein, versucht der fli4l diesen httpd immer wieder zu starten. Das schlägt fehl, weil der Port schon vom Admin-Interface oder einem anderen Dienst belegt ist. Das kann nur auf der Konsole oder in einem eingeschalteten Log gesehen werden. Man merkt es daran, dass C3SURF nicht funktionieren wird, fli4l hohe CPU-Last erzeugt und langsam zu laufen scheint.

**C3SURF\_HTTPD\_LISTENIP** Standard-Einstellung: C3SURF\_HTTPD\_LISTENIP='Host OR IPAdresse'

Gibt die lokale IP an, an die sich das Interface für die Anmeldung binden soll, entweder IP-Adresse oder @hostname. Hierhin werden http Anfragen der Clients bei Bedarf (also wenn sie nicht angemeldet sind) umgeleitet. So kommen die Anwender dann schnell auf die Anmeldeseite.

#### Beispiele:

```
C3SURF_HTTPD_LISTENIP='@wifi-router'    # Angabe eines Hostnamens
C3SURF_HTTPD_LISTENIP='192.168.11.3'    # Angabe einer IP-Adresse
C3SURF_HTTPD_LISTENIP='IP_NET_1_IPADDR' # Angabe einer IP-Adress-Variablen
```

Der http-Dienst für C3SURF wird immer an genau eine IP-Adresse gebunden.

### 1.3.1. Optionale Parameter OPT\_C3SURF

**C3SURF\_CONTROL\_SQUID** Standard-Einstellung: C3SURF\_CONTROL\_SQUID='no'

Mit dem Einfügen der Variablen C3SURF\_CONTROL\_SQUID='yes' wird die Kontrolle über squid erzwungen. Damit wird die C3SURF Portumleitung an den Anfang gesetzt, was auch Auswirkungen auf andere Pakete hat (z. B. openvpn).

Die Empfehlung ist 'no', wer z.B. squid verwendet sollte prüfen, ob nicht ungewollt noch andere Funktionen dadurch beeinflusst werden.

**C3SURF\_SLOPPY\_MAC** Standard-Einstellung: C3SURF\_SLOPPY\_MAC='no'

- C3SURF\_SLOPPY\_MAC='no'

(Standard) - wenn dieser Parameter nicht angegeben wurde, lasse Login nur mit MAC-Adressermittlung aus der ARP-Tabelle zu.

- C3SURF\_SLOPPY\_MAC='yes'

C3SURF akzeptiert auch MAC-Adressen die fehlen und nicht über die ARP-Tabelle ermittelbar sind. Wer hier 'yes' wählt sollte `C3SURF_CHECK_ARP='no'` (Seite 8) setzen. Sonst erfolgt die automatische Abmeldung (im Mittel nach einer Minute), weil der "countdown"-Prozess wegen fehlendem Eintrag in der ARP-Tabelle zur Abmeldung aufgefordert wird.

**C3SURF\_CHECK\_CURFEW** Standard-Einstellung: `C3SURF_CHECK_CURFEW='yes'`

Schalte automatisches Abmelden beim Erreichen der Sperrstunde an ('yes') oder ab ('no').

**C3SURF\_PORTAL\_DEFAULT\_LANG** Standard-Einstellung: `C3SURF_PORTAL_DEFAULT_LANG='de'`

Wertebereich: ein zweistelliger Ländercode (z. B. 'de', 'fr', 'en').

Legt die Standard-Sprache für die Anmeldeseite fest. Wird diese Variable weggelassen, wird 'de' angenommen.

Es sollte unter `~/opt/files/srv/www/c3surf/lang/` eine Datei namens `c3surf.<ländercode>` existieren. Derzeit werden 'de', 'fr', 'en' und 'it' mitgeliefert. Wer daraus für eine andere Sprache eine weitere Datei erstellt, möge diese an das fli4l-Team schicken.

**C3SURF\_PORTAL\_LANGUAGES**

Standard-Einstellung: `C3SURF_PORTAL_DEFAULT_LANG='de fr en it'`

Wertebereich: eine mit Leerzeichen getrennte Liste von immer zwei Buchstaben.

Legt fest, welche Sprachdateien für die Anmeldeseite auf das System übertragen werden sollen. Sollten hier zweistellige Kürzel stehen, zu denen keine Sprachdatei existiert, so wird bei der Generierung der Router-Images eine Warnung ausgegeben, dass zu dem Kürzel in der Liste keine Datei gefunden wurde und somit auch nichts kopiert wurde. Der Build-Prozess wird nicht abgebrochen.

### 1.4. Dokumentation der Funktion LOGINUSR für C3SURF

Stellt eine Anmeldung für Benutzer bereit. Damit kann nicht mehr jeder das Internet oder die Dienste des Routers nutzen. Eine Umschaltung im laufenden Betrieb ist technisch möglich aber derzeit nicht implementiert.

**Wichtig:** *Die ist keine echte Benutzeranmeldung, die Software substituiert jeden Benutzer auf eine Rechneradresse. Nach Ablauf der Quota wird dann nicht der Rechner (IP-Adresse) sondern der Benutzer geblockt.*

## 1.5. Konfiguration OPT\_LOGINUSER für C3SURF

**OPT\_LOGINUSR** Standard-Einstellung: OPT\_LOGINUSR='no'

OPT\_LOGINUSR='yes': echte Anmeldung verwenden (wird empfohlen)

LOGINUSR stellt eine echte Anmeldung (User/Password) zur Verfügung. Die Account Verwaltung erfolgt in der Config-Datei, Passwörter werden nur verschlüsselt übertragen.

### **LOGINUSR\_DELETE\_PERSISTENT\_DATA**

Standard-Einstellung: LOGINUSR\_DELETE\_PERSISTENT\_DATA='no'

LOGINUSR\_DELETE\_PERSISTENT\_DATA

Benutzerdaten auf einer Platte bleiben erhalten. Der Standardwert 'no' stellt dies für die Accountdaten sicher.

**Mit der Eingabe von 'yes' werden alle Benutzer-Accounts bei jedem Neustart gelöscht. Danach erfolgt eine Neuanlage der Accounts, wie unten definiert.**

Es wird empfohlen hier 'no' beizubehalten. Dann bleiben die Daten zu den Accounts erhalten, als da sind:

- Benutzer-Accounts
- Quota-Daten, wenn [C3SURF\\_SAVE\\_QUOTA='yes'](#) (Seite 7) gewählt ist (s.o.) (für einen einzelnen Account siehe: [LOGINUSR\\_ACCOUNT\\_x\\_OVERWRITE](#) (Seite 14))

**LOGINUSR\_ACCOUNT\_N** LOGINUSR\_ACCOUNT\_N='0'

LOGINUSR\_ACCOUNT\_N

Anzahl Accounts, Wert: Ganze Zahl.

Gibt die Anzahl der User-Accounts an.

**LOGINUSR\_ACCOUNT\_x\_USER** LOGINUSR\_ACCOUNT\_x\_USER='user1'

LOGINUSR\_ACCOUNT\_x\_USER

Username für die Anmeldung (muss zwingend definiert werden).

**LOGINUSR\_ACCOUNT\_x\_PWD** LOGINUSR\_ACCOUNT\_x\_PWD='user1\_secret'

LOGINUSR\_ACCOUNT\_x\_PWD

Passwort für die Anmeldung (muss zwingend definiert werden)

**LOGINUSR\_ACCOUNT\_x\_FORENAME** LOGINUSR\_ACCOUNT\_x\_FORENAME='Vorname'

LOGINUSR\_ACCOUNT\_x\_FORENAME

Vorname des Nutzers für die bessere Verwaltung (Optional, leer lassen erlaubt). Dieser Inhalt wird im Log und Admin-Interface angezeigt, so kann der Admin besser erkennen, wer gerade online ist.

**LOGINUSR\_ACCOUNT\_x\_SURNAME** LOGINUSR\_ACCOUNT\_x\_SURNAME='Nachname'

LOGINUSR\_ACCOUNT\_x\_SURNAME

Nachname des Nutzers für die bessere Verwaltung (Optional, leer lassen erlaubt). Dieser Inhalt wird im Log und Admin-Interface angezeigt, so kann der Admin besser erkennen, wer gerade online ist.

**LOGINUSR\_ACCOUNT\_x\_EMAIL** LOGINUSR\_ACCOUNT\_x\_EMAIL='usr1@home.de'

LOGINUSR\_ACCOUNT\_x\_EMAIL

E-Mail des Nutzers für die bessere Verwaltung (Optional, leer lassen erlaubt). Dieser Inhalt wird im Log und Admin-Interface angezeigt, so kann der Admin besser erkennen, wer gerade online ist.

**LOGINUSR\_ACCOUNT\_x\_OVERWRITE** LOGINUSR\_ACCOUNT\_x\_OVERWRITE='yes'

Optional:LOGINUSR\_ACCOUNT\_x\_OVERWRITE

Überschreibe persistente Nutzerdaten beim Router-Neustart.

Es kann ein Verzeichnis für persistente Daten angegeben werden. Dort werden die Daten für die Accounts gespeichert. Damit stehen diese Daten unverändert nach einem Reboot zur Verfügung. Mit dieser Option können der Benutzer-Account und alle zugehörigen persistenten Daten (Statistiken) überschrieben werden.

### 1.5.1. Optionale Parameter OPT\_LOGINUSR

**LOGINUSR\_ACCOUNT\_x\_TIME** LOGINUSR\_ACCOUNT\_x\_TIME='60'

Anzahl der Minuten nur für diesen Nutzer.

Fehlt dieser Parameter, so gilt [C3SURF\\_TIME](#) (Seite 7). Das Überschreiben macht natürlich nur Sinn, wenn [C3SURF\\_QUOTA='yes'](#) (Seite 5) eingestellt ist.

**LOGINUSR\_ACCOUNT\_x\_BLOCKTIME** LOGINUSR\_ACCOUNT\_x\_BLOCKTIME='240'

Sperrzeit nur für diesen Nutzer.

Fehlt dieser Parameter, so gilt [C3SURF\\_BLOCKTIME](#) (Seite 7). Das Überschreiben macht natürlich nur Sinn, wenn [C3SURF\\_QUOTA='yes'](#) (Seite 5) eingestellt ist.

**LOGINUSR\_ACCOUNT\_x\_COUNTER** LOGINUSR\_ACCOUNT\_x\_COUNTER='1'

Anzahl der Anmeldungen nur für diesen Nutzer.

Fehlt dieser Parameter, so gilt [C3SURF\\_COUNTER](#) (Seite 6). Das Überschreiben macht natürlich nur Sinn, wenn [C3SURF\\_QUOTA='yes'](#) (Seite 5) eingestellt ist.

**LOGINUSR\_ACCOUNT\_x\_CURFEW** LOGINUSR\_ACCOUNT\_x\_CURFEW='Liste Sperrstunden'

Format: (Liste von Sperrstunden 0-23 durch Leerzeichen getrennt)

Beispiel: LOGINUSR\_ACCOUNT\_x\_CURFEW='0 1 2 3 4 5 6 7 21 22 23'

Bedeutung: Eine Anmeldung ist nur zwischen 8:00-20:59 Uhr erlaubt. Die Anmeldung wird immer unterbunden, wenn der Nutzer sich innerhalb der Stunde (plus 0-59 Minuten), die in der Liste steht, versucht anzumelden.

Ist der Benutzer angemeldet und läuft in die Sperrstunde, so wird er ohne Warnung automatisch abgemeldet. Das Abmeldeverhalten kann durch den optionalen Parameter [C3SURF\\_CHECK\\_CURFEW](#) (Seite 12)='no' unterbunden werden.

Mit dieser Liste kann ein Zugang sehr flexibel eingeschränkt werden. Die Liste kann auch wie gewohnt im Webinterface verwaltet werden. Bei der Eingabe findet keine Prüfung der Liste statt. **Es sind nur die Zahlen von 0 bis 23 sinnvoll!**

Zugehöriger OPT\_C3SURF Parameter:

**C3SURF\_CHECK\_CURFEW** (Seite 12)='no'

- C3SURF\_CHECK\_CURFEW='no': schaltet automatisches Abmelden beim Erreichen der Sperrstunde ab.
- C3SURF\_CHECK\_CURFEW='yes' (Standard): wer bei Erreichen der Sperrstunde angemeldet ist, wird abgemeldet.

## 1.6. Dokumentation der Funktion VOUCHER für C3SURF

Das OPT\_C3SURF\_VOUCHER ermöglicht einen anonymen Zugang in das Internet. Es werden Gutscheine erstellt, die in unterschiedlichen Kategorien eingerichtet werden können. Das Opt kann dann über das Webinterface manuell oder automatisch verwaltet werden.

## 1.7. Konfiguration von OPT\_VOUCHER

**OPT\_C3SURF\_VOUCHER** OPT\_C3SURF\_VOUCHER='no'

Das Gutscheinsystem von Opt C3SURF\_VOUCHER aktivieren ('yes'), Standard ist 'no'. Gutscheine sind anonyme aber sichere Einmal-Accounts, die zur Anmeldung verwendet werden können. Voraussetzung ist die Einstellung **OPT\_LOGINUSR='yes'** (Seite 13).

Die Erzeugung und Löschung der Gutscheine übernehmen zwei nächtliche cron JOBS, welche jederzeit auch manuell(Admin-Interface) gestartet werden können. Im Folgenden wird erklärt wie diese Jobs verwaltet werden.

Alle neu generierten Gutscheine werden an eine Druckliste angehängt. Nur in der Druckliste ist das zum Gutschein gehörende Kennwort im Klartext gespeichert. Du kannst diese Liste jederzeit Herunterladen, Drucken oder Löschen. Nach dem Löschen der Liste kann das Kennwort nicht wieder ermittelt werden. Normal wird die Liste zuerst gedruckt und dann gelöscht. Es darf immer nur ein gedrucktes Exemplar eines Gutscheines geben. Die Druckfunktion ist in html implementiert, Seitenumbrüche werden leider nicht beachtet. Gutscheine, die durch Seitenwechsel nicht gedruckt werden, sollten vernichtet werden (allerdings verfallen sie sowieso durch Zeitablauf). Listen, die nicht gedruckt, sondern heruntergeladen wurden, können mit anderen Programmen ein eigenes Layout erhalten, welches dann auch Seitenwechsel sauber berücksichtigt.

**C3SURF\_VOUCHER\_N** C3SURF\_VOUCHER\_N='n'

Wertebereich: 0 und Natürliche Zahlen

Wie viele verschiedene Gutscheinkategorien sollen erzeugt werden? Wichtigstes Kriterium für Gutscheine ist die Laufzeit. Daneben gibt man noch die Anzahl der Gutscheine und deren Gültigkeit in Tagen an. Siehe auch die folgenden Variablen.

**C3SURF\_VOUCHER\_x\_TIME** C3SURF\_VOUCHER\_x\_TIME='30'

Wertebereich: Natürliche Zahlen

Laufzeit in Minuten (hier: 30) für einen Gutschein dieser Kategorie ('n' siehe oben).

**C3SURF\_VOUCHER\_x\_COUNT** C3SURF\_VOUCHER\_x\_COUNT='3'

Wertebereich: Natürliche Zahlen

Wie viele Gutscheine dieser Kategorie (in diesem Fall 3) sollen erzeugt werden?

**C3SURF\_VOUCHER\_x\_DAYS** C3SURF\_VOUCHER\_x\_DAYS='90'

Wertebereich: 0 und Natürliche Zahlen

Wie viele Tage soll der Gutschein ab seiner Erzeugung gültig sein (hier:90). Damit wird ein Verfallsdatum für diesen Gutschein erzeugt. Die Löschung erfolgt dann entweder manuell oder per cron-Job. Der Gutschein erlischt, wenn er das erste Mal verwendet wird.

**Wichtig:** '0' bedeutet, dass Gutscheine dieser Kategorie kein Verfallsdatum haben. Sie werden erst mit Benutzung oder wenn die Zeit komplett verbraucht wurde ungültig (wird auch durch C3SURF\_VOUCHER\_LIVES\_N beeinflusst). Sie können jedoch jederzeit im Admin-Interface des fli4l gelöscht werden.

### 1.7.1. Optionale Parameter OPT\_VOUCHER

**C3SURF\_VOUCHER\_x\_LIVES** C3SURF\_VOUCHER\_x\_LIVES='n'

Wertebereich(n): -1, 0, Natürliche Zahlen

Angabe von Stunden, die der Voucher nach der ersten Anmeldung noch gültig ist.

#### Sonderfälle:

- C3SURF\_VOUCHER\_x\_LIVES='-1'  
bis zum ursprünglich generierten Verfallsdatum aus C3SURF\_VOUCHER\_DAYS gültig
- C3SURF\_VOUCHER\_x\_LIVES='0'  
(Standard), bedeutet Voucher wird mit erster Anmeldung ungültig.
- C3SURF\_VOUCHER\_x\_LIVES='Natürl. Zahl'  
Anzahl der Stunden, die der Voucher nach erster Anmeldung weiter gültig ist - ggf. ein neues Verfallsdatum berechnen.

Diese Gutscheine werden nicht mit der ersten Anmeldung ungültig, sondern gelten 'n' Stunden weiter. Sobald der Gutschein benutzt wird, wird daraus ein zeitlich limitierter LOGINUSR-Account generiert oder es wird das Verfallsdatum des Vouchers neu berechnet. Dieser Account / Voucher darf sich beliebig oft an und wieder abmelden. Es wird das von LOGIN\_USR gewohnte Quota-System für diesen Account verwendet. Erst wenn die gesamte Zeit verbraucht ist oder wenn das Verfallsdatum (C3SURF\_VOUCHER\_DAYS\_N) erreicht wurde, wird dieser Account automatisch von C3SURF gelöscht.



**C3SURF\_VOUCHER\_DEL\_CRON** C3SURF\_VOUCHER\_DEL\_CRON='0 4 \* \* \*'

Wertebereich: 'cron-Syntax' oder 'never'

Der oben angegebene Wert ist der Standard, wenn diese Variable in der config-Datei 'c3surf.txt' fehlt. Standard: lösche täglich morgens um 4 Uhr alle verfallenen Gutscheine.

Die cron-Syntax ist einzuhalten und wird nicht geprüft. Zusätzlich kann der Wert 'never' verwendet werden. Dann wird der Job vom System überhaupt nicht eingeplant. Man kann im Admin-Interface jederzeit manuell alle verfallenen Gutscheine löschen lassen.

**C3SURF\_VOUCHER\_GEN\_CRON** C3SURF\_VOUCHER\_GEN\_CRON='15 4 \* \* \*'

Wertebereich: 'cron-Syntax' oder 'never'

Der oben angegebene Wert ist der Standard, wenn diese Variable in der config-Datei 'c3surf.txt' fehlt. Standard: generiere täglich morgens um 4:15 Uhr neue Gutscheine, falls weniger als C3SURF\_VOUCHER\_COUNT vorhanden sind.

Die cron-Syntax ist einzuhalten und wird nicht geprüft. Zusätzlich kann der Wert 'never' verwendet werden. Dann wird der Job vom System überhaupt nicht eingeplant. Man kann im Admin-Interface jederzeit manuell neue Gutscheine bis zur Menge

[C3SURF\\_VOUCHER\\_x\\_COUNT](#) (Seite 16) erzeugen lassen.

Alle neu generierten Gutscheine werden an eine Druckliste angehängt. Nur in der Druckliste ist das zum Gutschein gehörende Kennwort im Klartext gespeichert. Jeder Gutschein sollte nur einmal gedruckt werden. Die Liste sollte sofort nach dem Ausdruck oder Herunterladen gelöscht werden.

**C3SURF\_VOUCHER\_PRTUPDATE** Standard-Einstellung: C3SURF\_VOUCHER\_PRTUPDATE='no'

Wertebereich: 'yes' oder 'no'

Aktualisierung der Druckdatei. Meine Empfehlung: 'no'. Wer wenige Gutscheine im System hält und die Druckdatei nach dem Ausdruck oder Herunterladen nicht löschen möchte, kann mit 'yes' eine Aktualisierung der Druckdatei beim Verbrauch von Gutscheinen einstellen. Bei der Wahl von 'yes' werden benutzte Gutscheine auch aus der Druckdatei gelöscht. Das benötigt Ressourcen auf dem Router.

**C3SURF\_VOUCHER\_USRLEN** Standard-Einstellung: C3SURF\_VOUCHER\_USRLEN='12'

Wertebereich: '1-16'

Zeichenlänge für Gutscheinaccount festlegen, ab 8 Zeichen werden '-' als Trenner eingebaut, die auch eingegeben werden müssen. Es werden immer vier Zeichen grup-

piert. Der Maximalwert ist 16.

**C3SURF\_VOUCHER\_USRCAP** Standard-Einstellung: C3SURF\_VOUCHER\_USRCAP='random'

- 'yes' : nur Großbuchstaben
- 'no' : nur Kleinbuchstaben
- 'random' : zufällige Wechsel von Groß- Kleinschreibung (Empfehlung)

Mit dieser Variable wird festgelegt ob Groß- oder Kleinbuchstaben im Benutzernamen verwendet werden sollen. Der Wert 'random' (empfohlen) bewirkt eine zufällige Auswahl.

**C3SURF\_VOUCHER\_PWDLEN** Standard-Einstellung: C3SURF\_VOUCHER\_PWDLEN='6'

Wertebereich: 1-12

Zeichenlänge für das Gutschein-Password.

**C3SURF\_VOUCHER\_PWDMOD** Standard-Einstellung: C3SURF\_VOUCHER\_PWDMOD='3'

Wertebereich: 1-5

Modulo für zufällige Verlängerung des Passwortes. Max: 5 (die Werte 0, 1, 2, 3, 4), Min 1 (der Wert 0). Es wird bei der Password-Generierung das Password zufällig um die möglichen Werte verlängert. Damit ergeben sich per default Password-Längen zwischen 6 und 8. Maximal einstellbar sind Password-Längen zwischen 12 und 16, das ist sicher genug mit zufälliger Groß- und Kleinschreibung.

**C3SURF\_VOUCHER\_PWD CAP** Standard-Einstellung: C3SURF\_VOUCHER\_PWD CAP='random'

- 'yes' : nur Großbuchstaben
- 'no' : nur Kleinbuchstaben
- 'random' : zufälliger Wechsel von Groß- und Kleinschreibung (Empfehlung)

Mit dieser Variablen wird festgelegt ob Groß- oder Kleinbuchstaben im Passwort verwendet werden sollen. Der Wert 'random' (empfohlen) bewirkt eine zufällige Auswahl.

## 1.8. Dokumentation der Funktion Traffic für C3SURF

Das OPT\_C3SURF\_TRAFFIC ermöglicht "Power User" auszubremsen und in ihre Schranken zu weisen. Es wird das Datenvolumen in einem definierbaren Zeitintervall überwacht und ausgewertet. Die Konfiguration kann nach eigenen Bedürfnissen angepasst werden.

## 1.9. Konfiguration OPT\_C3SURF\_TRAFFIC

**OPT\_C3SURF\_TRAFFIC** Standard-Einstellung: OPT\_C3SURF\_TRAFFIC='no'

Die Angabe von 'yes' hier aktiviert das Traffic-Modul. Die weiteren Variablen sind im Folgenden beschrieben. Die Defaultwerte sind für einen DSL-6000 Anschluss ausgelegt

Mit den folgenden Variablen kann eingestellt werden in welcher Zeit welches Datenvolumen nicht überschritten werden darf. Dabei wird nicht zwischen Up- und Download unterschieden. Die Logik dieses Moduls ist so konzipiert, dass bei zweimaliger Überschreitung des Volumens in Folge die Abmeldung des Verursachers erfolgt und dieser mit der definierten Zeitstrafe (Blockzeit) belegt wird. Diese Einstellungen wirken global für alle C3SURF-Benutzer. Die Wahl der richtigen Parameter sollte von der vor Ort verfügbaren Bandbreite abhängen. Da keine Sperre bei einmaliger Überschreitung erfolgt, kann auch mal ein Betriebssystem-Update oder das normale Herunterladen größerer Datenmengen erfolgen. Sollte der Verbrauch der Bandbreite aber als "dauerhaft" erkannt werden wird eine Sperre aktiv.

Will man beispielsweise das gelegentliche Herunterladen von größeren Datenmengen erlauben, so muss bei der Wahl der Parameter aus der erlaubten Datenmenge und der verfügbaren Bandbreite eine Zeit kalkuliert werden, in der die Datenmenge herunterladbar sein soll.

### Beispiel:

Das Herunterladen einer Distributions-CD (700MB) würde im günstigsten Fall folgende Zeiten in Anspruch nehmen:

DSL-	1000	ca.	93	Minuten
DSL-	2000	ca.	47	Minuten
DSL-	6000	ca.	16	Minuten
DSL-	16000	ca.	6	Minuten

Die erlaubte Datenmenge (hier 700MB) sollte durch einen Wert kleiner (aber nahe an) 2 und größer 1 geteilt werden.

**Beispiel (konservativ):** 700MB / 1,9 = 386317473 Bytes

Das wäre die Anzahl Bytes, die in der oben kalkulierten Zeit maximal heruntergeladen werden darf. Ob es sinnvoll ist, solch ein hohes Volumen bei DSL-1000 oder DSL-2000 pro Nutzer zuzulassen, hängt auch von der Anzahl der erwarteten Nutzer ab.

Will man solche Datenmengen nicht zulassen, sondern maximal z. B. das Musikhören eines mp3-Streams oder einen kontinuierlichen Datenstrom von 128 kBit/s erlauben, so sollte man unabhängig vom DSL-Anschluss folgende Werte wählen: 16220160 Bytes pro 15 Minuten (ergibt sich aus  $128\text{kBit/s} * 1024 / 8\text{Bit} = 16384 \text{ Bytes/s} * 60 = 983040 \text{ Bytes/min} * 15\text{min} = 14745600 \text{ Bytes} * 1,1 = 16220160 \text{ Bytes}$  (pro 15 min)). Da es sich um einen kontinuierlichen Datenstrom handelt darf nicht geteilt werden, denn diese Last ist ja immer zulässig. Hier ist es sinnvoll noch 10% Sicherheitsaufschlag zu kalkulieren, da neben der reinen Datenmenge auch noch

andere Informationen transportiert werden müssen. Daher wurde der errechnete Wert von 14745600 Bytes noch mit 1,1 multipliziert.

Im Folgenden werden die Variablen vorgestellt mit Default-Werten für das hier angeführte Beispiel mit dem gelegentlichen CD-Download an einem DSL-6000 Anschluss.

**C3SURF\_TRAFFIC\_BYTES** C3SURF\_TRAFFIC\_BYTES='386317473'

Wertebereich: natürliche Zahlen

Legt die Anzahl der Bytes fest, die maximal in der Zeit [C3SURF\\_TRAFFIC\\_MINUTES](#) (Seite 20) heruntergeladen werden darf. Hier als Beispiel der 1,9te Teil einer 700MB CD. Für das Beispiel mp3-Hören mit 128kBit ist hier 16220160 einzutragen.

**C3SURF\_TRAFFIC\_MINUTES** C3SURF\_TRAFFIC\_MINUTES='16'

Wertebereich: natürliche Zahlen

Legt die Zeit in Minuten fest, die zwischen zwei Messungen des Datenvolumens verstreicht. Wird nach der hier abgelaufenen Zeit eine Überschreitung festgestellt, so wird der Verursacher zunächst temporär gespeichert. Wird bei der nächsten Messung wieder eine Überschreitung festgestellt, so erfolgt automatisch die Abmeldung und Sperrung (für [C3SURF\\_TRAFFIC\\_BLOCKTIME](#) (Seite 20) Minuten). Wird bei der zweiten Messung keine Überschreitung mehr festgestellt, wird die temporäre Speicherung wieder gelöscht.

Für das mp3-Beispiel ist hier '15' einzustellen.

**C3SURF\_TRAFFIC\_BLOCKTIME** C3SURF\_TRAFFIC\_BLOCKTIME='60'

Wertebereich: ganze Zahlen

Legt die Zeit in Minuten fest, die ein Zugang nach Überschreitung des Traffic-Limits gesperrt wird.

## 1.10. Allgemeines zu C3SURF

### 1.11. fli4l Webinterface

**Rechte:** c3surf:view, admin

- view: Den Eintrag im Admin Menü anzeigen
  - admin: Für die Nutzung der Funktionen im Web-Interface.
- Httpd-User mit dem Recht “all” haben auch hier alle Rechte.
- Das OPT C3SURF trägt sich in der Weboberfläche unter “Opt” als “c3Surf” ein.

### 1.12. Funktionsweise

Mit c3surf können Netze oder einzelne Hosts spezifiziert werden, die nach dem Systemstart zunächst gesperrt sind. Durch eine formlose Registrierung über das Webinterface können Benutzern Freischaltungen auf Zeit vornehmen.

## 1. Dokumentation des Paketes C3SURF

Ist die LOGINUSR - Option aktiviert, dann können sich nur Personen anmelden, die einen gültigen Zugang mit Benutzernamen und Passworte besitzen.

Über das Admin-Interface des Routers können Benutzer oder MAC-Adressen angezeigt, ausgeloggt sowie temporär oder dauerhaft gesperrt werden. Die Sperrung betrifft immer nur die Anmeldung über c3Surf und wird von c3Surf verwaltet. Kommt der Rechner über ein anderes interface an den Router, hat die Sperre keine Wirkung.

Die Anmeldung erfolgt durch Vornamen, Namen und E-Mail-Adresse oder durch User/Passwort. Nach Ablauf einer eingestellten Zeit wird der Zugang wieder gesperrt und kann durch neue Anmeldung wieder freigeschaltet werden.

Die Anmeldeseite kann auch für die Benutzer gesperrt werden (siehe FreeSurf bzw. LoginUsr im OPT-Menue des Webinterfaces).

Das alles kann im Admin-Teil des Webinterfaces nachvollzogen werden.

Will man bestimmte Rechner dauerhaft freischalten, so kannst dies im Web-Interface erfolgen. Siehe dazu die ARP-Liste oder die DHCP-Leases.

Jede Nutzung kann mit Quotas versehen werden. Damit kann die Nutzung in der Zeit eingeschränkt werden. Mit den Parametern "-TIME", "-BLOCKTIME" und "-COUNTER" lässt sich dabei sehr viel einstellen, auch benutzerbezogen.

Beispiele:

Time	Blocktime	Counter	Quota (C3SURF_QUOTA='yes')
60	-1	0	60 Min Zeit, keine Sperre nach Ablauf, mit jeder Anmeldung läuft die Zeit (Parkuhrprinzip)
60	240	0	60 Min Zeit, danach für 240 gesperrt, mit jeder Anmeldung läuft die Zeit (Parkuhrprinzip = Geld rein, Zeit läuft ohne Unterbrechungsmöglichkeit)
60	0	-1	60 Min Zeit, nach Ablauf der Zeit wird der Zugang bis 00:00 Uhr gesperrt, beliebige An- Abmeldungszahl (kein Parkuhrprinzip)
60	-1	1	60 Min Zeit, keine Sperre nach Ablauf der Zeit, die Zeit kann 1x unterbrochen werden
60	-1	-1	60 Min Zeit, keine Sperre nach Ablauf der Zeit, beliebig viele Unterbrechungen möglich
600	10080	-2	10 Stunden innerhalb einer Woche mit beliebig vielen Unterbrechungen
0	-1	0	Unendliche Zeit mit jeder Anmeldung, keine Sperre nach Ablauf der Zeit

## 1.13. Namensauflösung - DNS

**Wichtig:** Der fli4l muss als DNS-Server bei den Clients eingetragen sein und muss befähigt sein Namen aufzulösen. Dazu

- benötigt er einen “Forward” auf den DNS-Server des Netzes oder
- er ist selbst der DNS-Server und kann ggf. automatisch Verbindungen aufbauen.

Sonst gibt es Probleme automatisch auf die Anmeldeseite umzuleiten. Die kann aber immer noch manuell durch die Eingabe ihrer URL aufgerufen werden.

## 1.14. Sonstiges zu C3SURF

### 1.14.1. Warnung

**Wichtig:** Ohne `OPT_LOGINUSR='yes'` (Seite 13) ist es jeder Person möglich, die für ihren Rechner eine IP-Adresse vom Router zugewiesen bekommen hat (z. B. aus einem offenen WLAN), einen freien Zugriff auf das Internet und die nicht geblockten Dienste des Routers zu bekommen. c3Surf unterstützt beim Blocken der Dienste, ist aber kein Ersatz für eine ordentliche Konfiguration der Firewall in `base.txt`.

### 1.14.2. Empfehlung

**Wichtig:** Der Router sollte für alle Fälle über eine Recovery-Version verfügen. Mit einer unglücklichen Konfiguration kann man sich komplett aussperren.

### 1.14.3. Fehler

Fehlerbeschreibungen können mit Config-Info in einer der fli4l-Newsgruppen <http://www.fli4l.de/hilfe/newsgruppen-forum/> gepostet werden.

#### 1.14.4. Lizenz

Diese Software wird unter den Bedingungen der GNU General Public License in Version 2 oder folgende veröffentlicht. Damit ist diese Software frei für Benutzer, Entwickler und Firmen. Es ist guter Stil, wenn Urheber in einer weiteren Verwertung oder Veröffentlichung genannt werden. Das gilt besonders für freie Werke.

#### 1.14.5. Literatur

Wer gerne sein Netz für andere zur Verfügung stellt, der sollte sich auch einmal mit der rechtlichen Situation auseinander setzen.

Es gibt eine unter CC stehende Arbeit dazu:

Rechtsfragen offener Netze:

<http://digbib.ubka.uni-karlsruhe.de/volltexte/1000007749>

Autor: Mantz, Reto

Reihe: Schriften des Zentrums für Angewandte Rechtswissenschaft / ZAR

Zentrum für Angewandte Rechtswissenschaft, Universität Karlsruhe (TH)

Band: 8

Verlag: Universitätsverlag Karlsruhe

ISBN: 978-3-86644-222-1

Erschienen: 10.04.2008

# A. Anhang zum Paket C3SURF

Opt und Doku:	07. Januar 2008	Frank Saurbier	<a href="mailto:c3surf@arcor.de">mailto:c3surf@arcor.de</a>
Doku-TeXSatz:	01. April 2009	Helmut Backhaus	<a href="mailto:helmut.backhaus@gmx.de">mailto:helmut.backhaus@gmx.de</a>
Übergabe:	01. Mai 2010	fli4l-Team	<a href="mailto:team@fli4l.de">mailto:team@fli4l.de</a>

## A.1. Tips zu anderen Opts

### A.1.1. cpmvrmllog Config

Beispiel für das C3SURF-Logverzeichnis, mit restart des mini\_httpd

```
# archive C3SURF log dir
# einmal im Monat am 1. um 01:30
# maximal 12 Archive aufbewahren
CPMVRMLOG_n_ACTION='move'
CPMVRMLOG_n_SOURCE='/var/log/c3surf/c3surf_*.log'
CPMVRMLOG_n_DESTINATION='/data/Archive/log/c3surf'
CPMVRMLOG_n_CUSTOM='/usr/local/bin/c3surf_kill_httpd.sh'
CPMVRMLOG_n_MAXCOUNT='12'
CPMVRMLOG_n_CRONTIME='30 1 1 * *'
```

### A.1.2. Samba ohne Anmeldung erlauben

Man nehme das opt\_usercmd und trage dort folgendes ein.

```
USERCMD_BOOT_N='3'
USERCMD_BOOT_1='/sbin/iptables -I c3surf\_control 1 -v -p udp --dport
137:138 -j RETURN' # samba thru c3surf
USERCMD_BOOT_2='/sbin/iptables -I c3surf\_control 1 -v -p tcp --dport
455 -j RETURN' # samba thru c3surf
USERCMD_BOOT_3='/sbin/iptables -I c3surf\_control 1 -v -p tcp --dport
139 -j RETURN' # samba thru c3surf
```

Durch hinzufügen der Option `-d IPSambaHOST` kann die jeweilige Regel noch um den Zielrechner erweitert werden.



Damit werden die Samba Ports normal durch die Forward-Chain geleitet und nicht mehr von C3SURF geblockt. Sollten in der Forward-Chain samba Weiterleitungen verboten sein, so ändern diese Eintragungen nichts daran.

Es gelten also immer noch die Einstellungen in base.txt.

### A.1.3. Migration aus Vorgängerversionen

- Migration zur Version 2.3.1 (von 2.3.0)
  - Neue Variablen. Da es sich nur um optionale Variablen handelt, ist die Bearbeitung nicht zwingend erforderlich. Der neue Bereich ist in der config.txt so
  - “# + new 2.3.1 + begin ————— delete this line” gekennzeichnet.
  - Das Voucherformat hat sich geändert, alte Voucher können weiter verbraucht werden, sie werden aber bei der Generierung von neuen Vouchern nicht als existent erkannt. Wer es sauber haben will, sollte alle Voucher löschen und dann neu erzeugen.
- Migration zur Version 2.3.0 (von 2.2.2)
  - Will man keine Gutscheine nutzen, sind keine Änderungen an der Konfiguration nötig.
  - Bearbeite die neue Variablen für das OPT\_C3SURF\_VOUCHER, sofern man die Gutscheinfunktion nutzen möchte.
  - Der neue Bereich ist in der config.txt so
  - “# + new 2.3.0 + begin ————— delete this line” gekennzeichnet.
- Migration zur Version 2.2.2 (von 2.2.1)
  - Bearbeite die neue Variablen. Sie sind in der config.txt so
  - “# + new 2.2.2 + begin ————— delete this line” gekennzeichnet.
  - C3SURF\_CONTROL\_SQUID: optional zur Kontrolle von squid, da squid nicht den Konventionen entspricht ist es vorläufig.
  - Die Variablen zum überschreiben der Quota-Defaults bei LOGINUSR\_ACCOUNT sind jetzt optional
- Migration zur Version 2.2.1 (von 2.2.0)

### A. Anhang zum Paket C3SURF

- Bearbeite die neuen Variablen. Sie sind in der config.txt so
- “# + new 2.2.1 + begin ————— delete this line” gekennzeichnet.
- C3SURF\_WORKON\_TMP: Empfehlung für Festplattenschlaf 'yes' sonst 'no' auch bei FLASH Medien (s.u.).
- C3SURF\_SAVE\_QUOTA: Empfehlung 'yes' (s.u.).
- Migration zur Version 2.2.0 (von 2.1.0)
  - Bearbeite die neue Variable “C3SURF\_CHECK\_ARP” in der config nach (Empfehlung: 'yes', s.u.). Sie ist in der config.txt so
  - “# + new 2.2.0 + begin ————— delete this line” gekennzeichnet.
- Migration zur Version 2.1.0 (von früheren Versionen)
  - Bearbeite die neuen Variablen. Sie sind in der config.txt so
  - “# + new 2.1.0 + begin ————— delete this line” gekennzeichnet.
  - Die MAC-Blackliste (so Du eine gepflegt hast) musst Du manuell ins Verzeichnis “C3SURF\_PERSISTENT\_PATH” kopieren.
  - Das Format der c3surf\_login.log wurde um eine Spalte erweitert. Am besten die alte log sichern und in C3SURF\_LOG\_PATH löschen.

# Index

C3SURF\_BLOCK\_PORT\_N, [10](#)  
C3SURF\_BLOCK\_PORT\_x, [10](#)  
C3SURF\_BLOCKTIME, [7](#)  
C3SURF\_CHECK\_ARP, [8](#)  
C3SURF\_CHECK\_CURFEW, [12](#)  
C3SURF\_CONTROL\_HOST\_OR\_NET\_-  
N, [8](#)  
C3SURF\_CONTROL\_HOST\_OR\_NET\_-  
x, [8](#)  
C3SURF\_CONTROL\_PORT\_N, [9](#)  
C3SURF\_CONTROL\_PORT\_x, [9](#)  
C3SURF\_CONTROL\_SQUID, [11](#)  
C3SURF\_COUNTER, [6](#)  
C3SURF\_DOLOG\_HTTPD, [4](#)  
C3SURF\_DOLOG\_INVALID, [4](#)  
C3SURF\_DOLOG\_LOGIN, [4](#)  
C3SURF\_DOLOG\_PAGE, [4](#)  
C3SURF\_HTTPD\_LISTENIP, [11](#)  
C3SURF\_HTTPD\_PORT, [10](#)  
C3SURF\_LOG\_PATH, [4](#)  
C3SURF\_PERSISTENT\_PATH, [4](#)  
C3SURF\_PORTAL\_DEFAULT\_LANG, [12](#)  
C3SURF\_PORTAL\_LANGUAGES, [12](#)  
C3SURF\_QUOTA, [5](#)  
C3SURF\_SAVE\_QUOTA, [7](#)  
C3SURF\_SLOPPY\_MAC, [11](#)  
C3SURF\_TIME, [7](#)  
C3SURF\_TRAFFIC\_BLOCKTIME, [20](#)  
C3SURF\_TRAFFIC\_BYTES, [20](#)  
C3SURF\_TRAFFIC\_MINUTES, [20](#)  
C3SURF\_VOUCHER\_DEL\_CRON, [16](#)  
C3SURF\_VOUCHER\_GEN\_CRON, [17](#)  
C3SURF\_VOUCHER\_N, [15](#)  
C3SURF\_VOUCHER\_PRTUPDATE, [17](#)  
C3SURF\_VOUCHER\_PWD CAP, [18](#)  
C3SURF\_VOUCHER\_PWDLEN, [18](#)  
C3SURF\_VOUCHER\_PWDMOD, [18](#)  
C3SURF\_VOUCHER\_USRCAP, [18](#)  
C3SURF\_VOUCHER\_USRLEN, [17](#)  
C3SURF\_VOUCHER\_x\_COUNT, [16](#)  
C3SURF\_VOUCHER\_x\_DAYS, [16](#)  
C3SURF\_VOUCHER\_x\_LIVES, [16](#)  
C3SURF\_VOUCHER\_x\_TIME, [15](#)  
C3SURF\_WORKON\_TMP, [5](#)  
LOGINUSR\_ACCOUNT\_N, [13](#)  
LOGINUSR\_ACCOUNT\_x\_BLOCKTIME,  
[14](#)  
LOGINUSR\_ACCOUNT\_x\_COUNTER, [14](#)  
LOGINUSR\_ACCOUNT\_x\_CURFEW, [14](#)  
LOGINUSR\_ACCOUNT\_x\_EMAIL, [13](#)  
LOGINUSR\_ACCOUNT\_x\_FORENAME,  
[13](#)  
LOGINUSR\_ACCOUNT\_x\_OVERWRITE,  
[14](#)  
LOGINUSR\_ACCOUNT\_x\_PWD, [13](#)  
LOGINUSR\_ACCOUNT\_x\_SURNAME, [13](#)  
LOGINUSR\_ACCOUNT\_x\_TIME, [14](#)  
LOGINUSR\_ACCOUNT\_x\_USER, [13](#)  
LOGINUSR\_DELETE\_PERSISTENT\_DATA,  
[13](#)  
OPT\_C3SURF, [3](#)  
OPT\_C3SURF\_TRAFFIC, [19](#)  
OPT\_C3SURF\_VOUCHER, [15](#)  
OPT\_LOGINUSR, [13](#)