Package C3SURF - Admission Control Version 2.3.1

for fli4l Version 3.10.3

Frank Saurbier
email: c3surf@arcor.de
Tex Document: Helmut Backhaus
email: helmut.backhaus@gmx.de

The fli4l-Team
email: team@fli4l.de

July 26, 2015

Contents

1. Documentation For Package C3SURF

1.1. Introduction

With C3SURF you can create an open, unencrypted network/WiFi. For legal reasons, however, you should control who uses the network. C3SURF allows an informal registration to the network. The package is based on "opt_onco" (Copyright (c) 2001-2007 Michael Mattes). By using OPT_LOGINUSR an "almost" real login can be realized. C3SURF can generate vouchers and a rudimentary (experimental) control function to suppress excessive downloads is integrated as well.
It may be defined, which hosts or entire networks are managed by C3SURF. These are initially blocked on router startup and the http requests are sent to the C3SURF login page. After registering an account on the login page, usage is allowed on a time basis. Everything will be logged and can be controlled via the web interface of C3SURF.

1.2. Notes On Installation

- As always with opt-packets for the fli4l:
  - unpack opt_c3surf_<version>.tar.gz to the fli4l directory (Build-PC).
  - adapt c3surf.txt to your own needs.
  - add the rights 'c3surf:view,admin' to httpd.txt (if needed).
  - generate a new fli4l build.

Important: fli4l has to be configured as the DNS server on all clients and should be able to perform name resolution. To accomplish this

- **a "Forward" to the DNS server of the net is needed or**
- **fli4l itself is the DNS server and may establish connections automatically.**

Otherwise problems may arise to redirect requests to the login page. In all cases the page may also be accessed by entering its URL.

1.3. Configuration OPT_C3SURF

OPT_C3SURF Default Setting: `OPT_C3SURF='no'`

Activate or deactivate the package.

C3SURF_LOG_PATH Default Setting: `C3SURF_LOG_PATH='/var/log/c3surf'`

Defines the directory for C3SURF's log files. On router shutdown the log files should be saved to a persistent medium or the path can be set here, if you want to keep the files. The path must exist on the permanent medium.

Important: *'c3surf_mac.blacklist' resides in the persistent directory* *C3SURF_PERSISTENT_PATH (Page 4).* *An own blacklist has to be copied there. The scope of the protocol is defined below.*

C3SURF_DOLOG_LOGIN Default Setting: `C3SURF_DOLOG_LOGIN='yes'`

Logging of Login/Logout: c3surf_login.log (default: 'yes')

C3SURF_DOLOG_INVALID Default Setting: `C3SURF_DOLOG_INVALID='yes'`

Logging of invalid logins: c3surf_invalid.log (default: 'yes'). If `OPT_LOGINUSR` (Page 12) is set to 'yes', invalid logins can not be logged.

C3SURF_DOLOG_PAGE Default Setting: `C3SURF_DOLOG_PAGE='no'`

Logging of accesses to the html page: c3surf_page.log (default: 'no'). Each access to the login page will be logged. The page log grows fast and thus is only recommended for the "curious".

C3SURF_DOLOG_HTTPD Default Setting: `C3SURF_DOLOG_HTTPD='no'`

Logging of all accesses to mini_httpd: c3surf_httpd.log (default: 'no').

Important: *In addition start the log function of the Mini-httpd (use only for tests or debugging). When turned on, it is advisable to regularly check the log and delete it, it quickly gets quite large.*

opt_cpmvrmlog: `http://extern.fli4l.de/fli4l_opt-db3/search.pl?pid=427` may be used for regular saving. The mini_httpd has to be restarted afterwards for correct logging. The script `/usr/local/bin/c3surf_kill_httpd.sh (Config example in appendix) exists for this purpose.` (Page 23)

C3SURF_PERSISTENT_PATH Adapt in any case, recommendation: '/var/lib/persistent/c3surf'

Defines the directory for files that should be preserved after a reboot or poweroff. Ideally, this points to a hard disk or CF card ('/var/lib/persistent/c3surf'). A directory in the RAM disk may be selected as well (eg in order to minimize access to the medium). In this case the directory should be copied to the disk from time to time (eg by opt_cpmvrmlog) because the data would be lost after a reboot, crash or power loss.

What is saved here:

MAC blacklists:

'c3surf_mac.blacklist', will be created when needed (see Admin Interface). Blocking of a MAC address is solved via an own file and not with the packet filter, because large amounts of entries may cause problemes there. Don't forget: blocked MAC addresses keep average users away from your net, which is enough for normal usecases, but not professionals. The MAC blacklist only prevents the login via C3SURF / loginusr, there are no direct blocks in the firewall.

User data:

<userloginname>.data (i.e. 'frank.data'), these files contain data on the user such as first and lastname, E-mail address, statistics and quotas. Persistant user data allows to avoid recreating user data files on every startup. This means: if for user "frank" a file 'frank.data' exist on system start the settings in the config file will be ignored.

Overwriting of user data may be forced by `LOGINUSR_ACCOUNT_x_OVERWRITE='yes'` (Page 13). By `LOGINUSR_DELETE_PERSISTENT_DATA='yes'` (Page 12), all "*.data" files will be deleted on reboot.

C3SURF_WORKON_TMP Default Setting: `C3SURF_WORKON_TMP='no'`

If `C3SURF_PERSISTENT_PATH` (Page 4) is set, you may specify 'yes' here. On system start persistent data will then be copied from the harddisk to the directory C3SURF_TMP_PATH and only be accessed there. Accesses to the harddisk by C3SURF only will occur if the admin writes data to persistent files.

Important: *Persistant data is:*

- *User accounts*
- *MAC blacklist*
- *System lock files (blocking of logins)*

For FLASH memory specify 'no' here, because in normal use C3SURF will only read files. Write accesses are only caused by the admin.

C3SURF_QUOTA Default Setting: `C3SURF_QUOTA='no'`

If the access should be limited, enter 'yes' here. Access is blocked for an IP address for `C3SURF_BLOCKTIME` (Page 7) minutes after reaching time limit or the maximum registration counter. Default value is 'yes'.

Important: *Individual -TIME, -BLOCKTIME and -COUNTER for LOGIN_USR accounts are activated ('yes') or deactivated ('no') by this variable.*

C3SURF_COUNTER Default Setting: `C3SURF_COUNTER='0'`

Specifies the number of possible interruptions within the surftime.

Important: *A multitude of interruptions for (Logout/Login) may be defined. If i.e. '1' is specified here the user may logout and login once within the surftime which corresponds to two registrations in this time. On the following registration the user gets the time difference left from C3SURF_TIME (Page 7).*

If in addition C3SURF_BLOCKTIME='0' (Page 7) is set the C3SURF_COUNTER (Page 6) will be reset at 0:00 o'clock the following day.

- With C3SURF_COUNTER='0'

  the value corresponds to the parking meter principle (money in, money gone, time runs: no interruption possible).

- With C3SURF_COUNTER= '-1'

  this function is deactivated = as many interruptions of surftime as you like are possible.

- With C3SURF_COUNTER='-2'

  as many interruptions of surftime as you like are possible (like '-1'), but blocking time countdown starts with the first login. In contrary to '-1', where blocking time starts after using the whole time. Since blocking time countdown runs simultaneously, the user will only be blocked when he consumes his or her quota too quickly.

Notes to the long-term contingent (C3SURF_COUNTER='-2'):
Hence you may combine i.e. 10 hours of online time C3SURFTIME(`C3SURF_TIME='600'`) with a blocking time of a week (`C3SURF_BLOCKTIME='10080'` (Page 7) : 60sec x 24h x 7days). This way the 10 hours may be used during one week. Those using all the time on the first day in one piece will have to wait for the rest of the week. After the blocking time 10 hours will be provided anew. Short: The user may use ten hours in one week, which he may spread in a meaningful manner over this timespan.

If the quota is not used within a week, no "Quota-Block" will occur. Then there is no waiting time. If the quota is used on the first day then the account is blocked for the remaining 6 days of the week. Applies also to `LOGINUSR_ACCOUNT_x_COUNTER` (Page 13).

Recommendation: `C3SURF_SAVE_QUOTA='yes'` (Page 7), to retain the values also after a normal reboot. On a power failure the values will be lost.

If `C3SURF_QUOTA='yes'` (Page 5), after reaching the counter a block corresponding to

C3SURF_BLOCKTIME (Page 7) is activated.

C3SURF_TIME Default Setting: C3SURF_TIME='60'

Number of minutes that an activation is valid.

The value '0' means an unlimited login (also applies for LOGINUSR_ACCOUNT_x_TIME).

Special case:

- C3SURF_TIME='0'

  Means unlimitited online time. The user himself should perform the logout. C3SURF will only logout the user if the computer was shut down and C3SURF_CHECK_ARP='yes' (Page 7) (default) was set.

C3SURF_BLOCKTIME Default Setting: C3SURF_BLOCKTIME='240'

Number of minutes an IP gets blocked if surftime was exceeded or the Admin performs a block via the Web interface. By this a computer may be blocked from the net for this time and thus usage is restricted. C3SURF_QUOTA='yes' (Page 5) has to be set in order to perform the block.

Special cases:

- C3SURF_BLOCKTIME='0'

  a block of the addresse resp. the user is preformed until 00:00 o'clock of the following day.

- C3SURF_BLOCKTIME='-1'

  no blocking will be performed.

Important: *Unblocking is performed with an accuracy of one minute.*

C3SURF_SAVE_QUOTA Default Setting: C3SURF_SAVE_QUOTA='yes'

Saves Quota values on shutdown and restores them on systemstart of the router. The temporary files of the quota-management will be written to C3SURF_PERSISTENT_PATH (Page 4) on normal shutdown and will be restored to the temporary directory on system start again. All actual user data will be preserved this way. An accidental shutdown will not be recoverable this way.

Important: *LOGINUSR_DELETE_PERSISTENT_DATA='no' (Page 12), should be set because otherwise this setting will delete all user accounts und their quota data.*

C3SURF_CHECK_ARP Default Setting: `C3SURF_CHECK_ARP='yes'`

Check in the countdown module whether an IP of a computer has vanished from the ARP table. Shut down computers may be recognized this way, but sometimes with a massive time delay.

C3SURF_CONTROL_HOST_OR_NET_N `C3SURF_CONTROL_HOST_OR_NET_N='0'`

Value: integer numbers.
How much and which IP ranges or hosts should be controlled by c3Surf? This affects forwarding to another net (FORWARD Chain).

C3SURF_CONTROL_HOST_OR_NET_x

`C3SURF_CONTROL_HOST_OR_NET_x='Netzwerk OR Host OR IP-Address'`

Controls all clients.

Important: *A complete net may be specified here for simplicity, e.g. WLAN. Then all wireless users need to use the login page. Also a reference to a host (@host) or an IP address may be specified. Who or what is entered here is redirected to the login page and the blocking rules defined below apply.*

Example:

```
C3SURF_CONTROL_HOST_OR_NET_1='IP_NET_3'       # Specify the net IP/MASK
C3SURF_CONTROL_HOST_OR_NET_2='@T8200'         # or host @HOST
C3SURF_CONTROL_HOST_OR_NET_3='192.168.13.11'  # or IP address
```

The next example is basically the same as the one above (IP_NET_3) if in "base.txt" the IP address has been set accordingly.

```
C3SURF_CONTROL_HOST_OR_NET_1='192.168.0.1/24' # controls all clients
```

For a computer to be excluded, you may either include all IP addresses individually in C3SURF.txt (i.e. create a list of all 256 addresses and leave one out), or you can use the CIDR notation (as above). Then IP groups have to be used causing less writing (8 rows instead of 255).

This may look as follows:

```
C3SURF_CONTROL_HOST_OR_NET_N='8'                # Number of hosts or nets
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
```

The computer with the IP '192.168.0.2' is able to do everything allowed by fli4l's firewall without registration.

C3SURF_CONTROL_PORT_N `C3SURF_CONTROL_PORT_N='0'`

Value: Integer numbers.
How much TCP ports of the routers should be controlled?

How much and which ports explicitely named should be controlled by c3Surf? IP ranges and hosts from above are affected.
C3SURF_CONTROL_HOST_OR_NET_N (Page 8). c3Surf controls these ports and frees them after successful login so that all services existing on this ports of the router may be used (INPUT-Chain).

C3SURF_CONTROL_PORT_x `C3SURF_CONTROL_PORT_x='port_nr'`

Port number and the access to the services of the router (fli4l) behind them are blocked until login. After successful registration, services can be used for the time provided.

Examples:

```
C3SURF_CONTROL_PORT_1='515' # i.e. lpdsrv (printer usable after login)
C3SURF_CONTROL_PORT_2='21'  # i.e. ftp - (note: ftp on the router!)

Other possible port adresses:
  21=ftp
  22=ssh
  5000=imonc
  5001=telmod
  8118=privoxy
  9050=tor
  3128=squid
  20000=mtgcapri
  80=http(Admin)
  515=lpdsrv
```

All depends on your own configuration. To all ports not mentioned here the rules from 'base.txt' apply. After registration, the rules of 'base.txt' are still valid. c3Surf is only a pre-chain to these rules until the login was performed successfully. So after registration all the rules are still obeyed. So you may, for example, deny access from WLAN to the wired network in 'base.txt'. This is also valid for users legitimated in WLAN by c3Surf.

C3SURF_BLOCK_PORT_N `C3SURF_BLOCK_PORT_N='0'`

Value: Integer numbers.

How much TCP ports of the routers should be blocked?

Hints:
Permanent blocking of services for nets and hosts mentioned above
C3SURF_CONTROL_HOST_OR_NET_N (Page 8). How much and which ports explicitely named should be blocked permanently by c3Surf? No access to the router's services behind those ports for hosts and/or computers of the blocked nets even not after login. This affects the INPUT-Chain. If you want to block certain services permanently, you should better do this with the parameters for the INPUT chain in 'base.txt'. Why:
Because these rules are not valid anymore if the parameter OPT_C3SURF='no' (Page 3) is set. If you deactivate C3SURF the rules defined here have to be transferred to the 'base.txt' if you want your blocks for the hosts or nets mentioned above to persist.

C3SURF_BLOCK_PORT_x C3SURF_BLOCK_PORT_x='port_nr'

Examples:

```
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 Default Setting: C3SURF_HTTPD_PORT='8080'

On which port and which IP address should the mini_httpd listen for login attempts? http queries from computers will be redirected to this address and port. Port 8080 is the default here.

The following should be considered when choosing the port number:

- You should not use the port from the httpd package (usually this is 80).
- The httpd for fli4l's web admin per default binds to all local IP's.
- also use no port number that is already used by another service.

If by mistake a port already in use is defined here, fli4l tries again and again to start httpd. This fails because the port is already occupied by the Admin Interface or another service. This can only be seen on the console or in the logs. You notice it because C3SURF will not work and fli4l generates high CPU load and appears to be running slowly.

C3SURF_HTTPD_LISTENIP Default Setting: `C3SURF_HTTPD_LISTENIP='Host OR IP-Address'`

Specifies the local IP to which the login interface will bind to, either IP address or @hostname. Http requests of clients will be redirected on demand (i.e., when they are not logged in). Hence, users come quickly to the login page.

Examples:

```
C3SURF_HTTPD_LISTENIP='@wifi-router'    # Hostname
C3SURF_HTTPD_LISTENIP='192.168.11.3'    # IP-address
C3SURF_HTTPD_LISTENIP='IP_NET_1_IPADDR' # IP-address-variable
```

The http service for C3SURF always binds to exactly one IP address.

1.3.1. Optional Parameters For OPT_C3SURF

C3SURF_CONTROL_SQUID Default Setting: `C3SURF_CONTROL_SQUID='no'`

By adding the variable C3SURF_CONTROL_SQUID='yes' the control over squid will be forced. The C3SURF port redirection will be set to the beginning which also affects other packages (i.e. openvpn).

Recommendation is 'no', those using i.e. squid should check, if no other functions are affected inadvertently by it.

C3SURF_SLOPPY_MAC Default Setting: `C3SURF_SLOPPY_MAC='no'`

- C3SURF_SLOPPY_MAC='no'

  (Standard) - if this parameter is not specified only allow login with MAC addresses from the ARP table.

- C3SURF_SLOPPY_MAC='yes'

  C3SURF accepts missing MAC addresses or those not contained in the ARP table. If you set this to 'yes' you should set `C3SURF_CHECK_ARP='no'` (Page 7). Else the automatic logout (in average after one minute) will be performed because the "countdown" process will fire due to a missing entry in the ARP table.

C3SURF_CHECK_CURFEW Default Setting: `C3SURF_CHECK_CURFEW='yes'`

Turn automatic logoff when reaching the curfew on (`'yes'`) or off (`'no'`).

C3SURF_PORTAL_DEFAULT_LANG Default Setting: `C3SURF_PORTAL_DEFAULT_LANG='de'`

Possible values: a two-characters country code (i.e. 'de', 'fr', 'en').

Sets the default language for the login page. If omitted, 'de' is assumed.

Under ~/opt/files/srv/www/c3surf/lang/ a file named c3surf.<countrycode> should exist. At the moment 'de', 'fr', 'en' and 'it' are supported. If you want to create a file for another language you may send it to the fli4l team for inclusion.

C3SURF_PORTAL_LANGUAGES

Default Setting: `C3SURF_PORTAL_DEFAULT_LANG='de fr en it'`

Value range: a list of two characters each, separated by spaces.

Specifies the language files that should be transferred to the system for the login page. If there is no language file corresponding to the two character shortcut here, a warning will be issued that no file was found for it and therefore nothing was copied. The build process is not aborted.

1.4. Documentation Of The Function LOGINUSR For C3SURF

Provides a login registration for users. It is no longer possible for everybody to use the Internet services of the router freely. Switching of operation modes is technically possible but not currently implemented.

Important: *This is no true user login, the software substitutes each user to a computer address. When the timeout is reached the user will be blocked, not the PC (IP address).*

1.5. Configuration Of OPT_LOGINUSER For C3SURF

OPT_LOGINUSR Default Setting: `OPT_LOGINUSR='no'`

OPT_LOGINUSR='yes': use true login (recommended)

LOGINUSR provides a true login (User/Password). Account management is done in the config file, passwords will be transferred only encrypted.

LOGINUSR_DELETE_PERSISTENT_DATA

Default Setting: `LOGINUSR_DELETE_PERSISTENT_DATA='no'`

LOGINUSR_DELETE_PERSISTENT_DATA
User data on a harddisk will survive reboots. The deault setting 'no' only preserves Account data.

With specifying 'yes' here all user accounts will be deleted on every reboot. Afterwards they will be recreated as described below.

It is recommended to keep the 'no' here to preserve all account data, i.e.:

- User Accounts
- Quotas, if `C3SURF_SAVE_QUOTA='yes'` (Page 7) is set (see above) (for defined accounts see: `LOGINUSR_ACCOUNT_x_OVERWRITE` (Page 13))

LOGINUSR_ACCOUNT_N `LOGINUSR_ACCOUNT_N='0'`

LOGINUSR_ACCOUNT_N
The number of accounts defined.

LOGINUSR_ACCOUNT_x_USER `LOGINUSR_ACCOUNT_x_USER='user1'`

LOGINUSR_ACCOUNT_x_USER
Username for login (mandatory).

LOGINUSR_ACCOUNT_x_PWD `LOGINUSR_ACCOUNT_x_PWD='user1_secret'`

LOGINUSR_ACCOUNT_x_PWD
Password for login (mandatory)

LOGINUSR_ACCOUNT_x_FORENAME `LOGINUSR_ACCOUNT_x_FORENAME='Vorname'`

LOGINUSR_ACCOUNT_x_FORENAME
First name of the user for better management (optional, may be empty). The content is shown in the logs and in the Admin interface to help the Admin to better recognize users being online at the moment.

LOGINUSR_ACCOUNT_x_SURNAME `LOGINUSR_ACCOUNT_x_SURNAME='Nachname'`

LOGINUSR_ACCOUNT_x_SURNAME
Last name of the user for better management (optional, may be empty). The content is shown in the logs and in the Admin interface to help the Admin to better recognize users being online at the moment.

LOGINUSR_ACCOUNT_x_EMAIL `LOGINUSR_ACCOUNT_x_EMAIL='usr1@home.de'`

LOGINUSR_ACCOUNT_x_EMAIL
E-Mail of the user for better management (optional, may be empty). The content is shown in the logs and in the Admin interface to help the Admin to better recognize users being online at the moment.

LOGINUSR_ACCOUNT_x_OVERWRITE `LOGINUSR_ACCOUNT_x_OVERWRITE='yes'`

Optional:LOGINUSR_ACCOUNT_x_OVERWRITE
Overwrite persistent user data on system restart.

A directoy for persistent data storing may be specified here to hold account data. This way the data is preserved after a reboot. With this option user accounts and all data for them (statistics) may be overwritten.

1.5.1. Optional Parameters For OPT_LOGINUSR

LOGINUSR_ACCOUNT_x_TIME `LOGINUSR_ACCOUNT_x_TIME='60'`

Time amount solely for this user, defined in minutes.

If omitted, `C3SURF_TIME` (Page 7) is valid. Overwriting only makes sense if `C3SURF_QUOTA='yes'` (Page 5) has been defined.

LOGINUSR_ACCOUNT_x_BLOCKTIME `LOGINUSR_ACCOUNT_x_BLOCKTIME='240'`

Locking time solely for this user.

If omitted, `C3SURF_BLOCKTIME` (Page 7) is valid. Overwriting only makes sense if `C3SURF_QUOTA='yes'` (Page 5) has been defined.

LOGINUSR_ACCOUNT_x_COUNTER `LOGINUSR_ACCOUNT_x_COUNTER='1'`

Number of logins solely for this user.

If omitted, `C3SURF_COUNTER` (Page 6) is valid. Overwriting only makes sense if `C3SURF_QUOTA='yes'` (Page 5) has been defined.

LOGINUSR_ACCOUNT_x_CURFEW `LOGINUSR_ACCOUNT_x_CURFEW='List of curfews'`

Format: (List of curfews 0-23 separated by spaces)

```
Example: LOGINUSR_ACCOUNT_x_CURFEW='0 1 2 3 4 5 6 7 21 22 23'
```

Meaning: A login is allowed only between 8:00-20:59. The login will always be denied if the user tries to login within the hour in the list (plus 0-59 minutes).

If the user is logged in and runs into a curfew, he will be logged out without a warning. The logout behavior can be prevented by specifying C3SURF_CHECK_CURFEW (Page 11)='no'.

By using this list access can be restricted very flexible. The list can also be managed in the Web interface. No checking of the list is performed. **Only the numbers from 0 to 23 make sense!**

OPT_C3SURF Parameters belonging here:
C3SURF_CHECK_CURFEW (Page 11)='no'

- C3SURF_CHECK_CURFEW='no': no automatic logout when reaching curfews is performed.
- C3SURF_CHECK_CURFEW='yes' (Standard): users will be logged out automatically when reaching curfews.

1.6. Documentation Of The Function VOUCHER For C3SURF

OPT_C3SURF_VOUCHER allows anonymous access to the Internet. There are vouchers created which can be arranged in various categories. The opt can then be managed manually or automatically on the Web Interface.

1.7. Configuration Of OPT_VOUCHER

OPT_C3SURF_VOUCHER `OPT_C3SURF_VOUCHER='no'`

Activate the voucher system of opt C3SURF_VOUCHER ('yes'), default is 'no'. Vouchers are anonymous yet secure single-use accounts that can be used for login. Requirement is the setting `OPT_LOGINUSR='yes'` (Page 12).

The creation and deletion of the vouchers is done by two nightly cron jobs which also can be started manually at any time (admin interface). The following explains how to manage these jobs.

All newly generated vouchers are attached to a print list. Only in the print list the password corresponding to the voucher is stored in plain text. You can download, print or delete this list at any time. After deleting the list, the password can not be recovered again. Normally the list is printed first and then deleted. There should only exist one printed copy of a voucher. the print function is implemented in html, page feeds are not taken into account. Vouchers which are not printed caused by a page feed should be destroyed (though they get invalid due to expiration anyway). Lists that were not printed but downloaded may get an own layout with other programs which also avoids the page feed caveat.

C3SURF_VOUCHER_N `C3SURF_VOUCHER_N='n'`

Value range: 0 and natural numbers

How many different voucher categories should be produced? The most important criterion for vouchers is the runtime. Next to it are the number of vouchers and their validity in days. See also the following variables.

C3SURF_VOUCHER_x_TIME `C3SURF_VOUCHER_x_TIME='30'`

Value range: natural numbers

Duration in minutes (here: 30) for a voucher of this category ('n' see above).

C3SURF_VOUCHER_x_COUNT `C3SURF_VOUCHER_x_COUNT='3'`

Value range: natural numbers

How many vouchers of this category (in this case 3) should be produced?

C3SURF_VOUCHER_x_DAYS `C3SURF_VOUCHER_x_DAYS='90'`

Value range: 0 and natural numbers

How many days do you want the voucher to be valid starting from its generation (here: 90). Thus, an expiration date for this coupon is generated. The deletion is then carried out either manually or via cron job. The voucher is void when it is first used.

Important: *'0' means that vouchers of this category have no expiration date. They only become invalid with use or if the time has been completely consumed (also affected by C3SURF_VOUCHER_LIVES_N). However they may be deleted at any time in the admin interface.*

1.7.1. Optional Parameters Of OPT_VOUCHER

C3SURF_VOUCHER_x_LIVES `C3SURF_VOUCHER_x_LIVES='n'`

Value range(s): -1, 0, natural numbers

Number of hours, in which the voucher is still valid after your first login.

Special cases:

- C3SURF_VOUCHER_x_LIVES='-1'

  valid until the expiration date originally generated with C3SURF_VOUCHER_DAYS
- C3SURF_VOUCHER_x_LIVES='0'

  (Standard), means voucher will become invalid with the first login.
- C3SURF_VOUCHER_x_LIVES='Natural number'

  Number of hours for which voucher is still valid after the first login - calculate a new expiration date if necesssary.

These vouchers will not become invalid with the first login, but are valid for 'n' more hours. Once the voucher is used, a time-limited LOGINUSR account is generated or

the expiry date of the voucher is recalculated. This account / voucher may login and logout for any number of times. The quota system of LOGIN_USR is used for this account. If the total time or the expiry date (C3SURF_VOUCHER_DAYS_N) is reached, C3SURF will automatically delete this account.

C3SURF_VOUCHER_DEL_CRON `C3SURF_VOUCHER_DEL_CRON='0 4 * * *'`

Value range: 'cron-Syntax' or 'never'

The above value is the default if the variable is missing in the config file 'c3surf.txt'. Default: delete all expired vouchers every morning at 4 o'clock.

Cron syntax must be obeyed and will not be verified. The value 'never' may be used in addition. Then the job is not scheduled by the system. In the admin interface all expired vouchers may be deleted manually at any time.

C3SURF_VOUCHER_GEN_CRON `C3SURF_VOUCHER_GEN_CRON='15 4 * * *'`

Value range: 'cron-Syntax' or 'never'

The above value is the default if the variable is missing in the config file 'c3surf.txt'. Default: generate new vouchers daily at 4:15 AM if less than C3SURF_VOUCHER_COUNT exist.

Cron syntax must be obeyed and will not be verified. The value 'never' may be used in addition. Then the job is not scheduled by the system. In the admin interface new vouchers may be generated manually at any time, up to the amount defined in `C3SURF_VOUCHER_x_COUNT` (Page 15).

All newly generated vouchers are attached to a print list. Only in the print list the password corresponding to the voucher is stored in plain text. Each voucher should be printed only once. The list should be deleted immediately after printing or downloading.

C3SURF_VOUCHER_PRTUPDATE Default Setting: `C3SURF_VOUCHER_PRTUPDATE='no'`

Value range: 'yes' or 'no'

Update of the print file. My recommendation: 'no'. If only a few vouchers are held in the system and the print file should not be deleted after printing or downloading, an update of the print file can be specified with 'yes' when vouchers are used. In the case of 'yes' used vouchers are also deleted from the print file. This requires resources on the router.

C3SURF_VOUCHER_USRLEN Default Setting: `C3SURF_VOUCHER_USRLEN='12'`

Value range: '1-16'

Set character length for voucher account, from 8 characters on '-' will be filled in as separators, which also must also be entered. There are always four characters grouped. The maximum value is 16.

C3SURF_VOUCHER_USRCAP Default Setting: `C3SURF_VOUCHER_USRCAP='random'`

- 'yes' : only capital letters
- 'no' : all lowercase
- 'random' : random change of upper and lower case (recommended)

This variable determines whether uppercase or lowercase letters should be used in the user name. The value `'random'` (recommended) causes a random selection.

C3SURF_VOUCHER_PWDLEN Default Setting: `C3SURF_VOUCHER_PWDLEN='6'`

Value range: 1-12

Character length for the voucher password.

C3SURF_VOUCHER_PWDMOD Default Setting: `C3SURF_VOUCHER_PWDMOD='3'`

Value range: 1-5

Modulo for random extensions of the password. Max: 5 (the values 0, 1, 2, 3, 4), Min 1 (the value 0). It is used randomly in the password generation to change the possible values. This results by default in password lengths from 6 to 8 characters. The maximum are password-lengths between 12 and 16 characters, in conjunction with random upper- and lowercase letters this is considered as safe.

C3SURF_VOUCHER_PWDCAP Default Setting: `C3SURF_VOUCHER_PWDCAP='random'`

- 'yes' : only capital letters
- 'no' : all lowercase
- 'random' : random change of upper and lower case (recommended)

This variable determines whether uppercase or lowercase letters should be used in the password. The value `'random'` (recommended) causes a random selection.

1.8. Documentation Of The Function Traffic For C3SURF

OPT_C3SURF_TRAFFIC makes it possible to throttle "Power Users". The data volume in a defined time interval will be monitored and evaluated. The configuration can be customized according to your needs.

1.9. Configuration Of OPT_C3SURF_TRAFFIC

OPT_C3SURF_TRAFFIC Default Setting: `OPT_C3SURF_TRAFFIC='no'`

Specifying 'yes' here activates the traffic module. The variables are described below. The defaults have been chosen with a DSL-6000 connection in mind.

With the following variables can be set in which time which data volume should not be exceeded. No distinction is made between upload and download. The logic of the module is designed in a way that if the volume is exceeded twice in a row - the offender will be blocked and this is done with the defined time penalty (block time). These settings are applied globally for all C3SURF users. Choosing the right parameters should depend on the bandwidth available on site. Since no lock at a single occurance is made, even an operating system update or the normal download of larger amounts of data is accepted. But if the bandwidth consumption is recognized as "permanently" a lock will become active.

If you want, for example, to allow the occasional downloading of large amounts of data a time has to be calculated out of the allowed amount of data and the available bandwidth in which the amount of data can be downloaded.

Example:

Downloading a distribution CD (700MB) would at best case take the following time to complete:

DSL-	1000	approximately	93	Minutes
DSL-	2000	approximately	47	Minutes
DSL-	6000	approximately	16	Minutes
DSL-	16000	approximately	6	Minutes

The allowed amount of data (here 700MB) should be divided by a value smaller (but near to) 2 and bigger than 1.

Example (conservative): 700MB / 1,9 = 386317473 Bytes

That would be the number of bytes that may be downloaded as a maximum in the time calculated above. Whether it makes sense to allow such a high volume per user for DSL-1000 and DSL-2000 depends also on the number of users expected.

If you don't want to allow such amounts of data, but for example allow listening to mp3 streams of music or allow a continuous data stream of 128 kbit/s, you should select the following values: 16220160 bytes per 15 minutes (results from 128kBit/s * 1024 / 8Bit = 16384 Bytes/s * 60 = 983040 Bytes/min * 15min = 14745600 Bytes * 1,1 = 16220160 Bytes (per 15 min)). Since this is a continuous data stream no devision should take place because this load is always permitted. Here it is useful to calculate a further 10% safety margin, since in addition to the pure amount of data other information must be transported too. Therefore, the calculated Value of 14745600 bytes is multiplied by 1.1.

In the following, the variables are presented with default values for the example given here for the occasional download of a CD with a DSL 6000 connection.

C3SURF_TRAFFIC_BYTES `C3SURF_TRAFFIC_BYTES='386317473'`

Value range: natural numbers

Specifies the number of bytes which may be downloaded in the maximum time `C3SURF_TRAFFIC_MINUTES` (Page 19). Here for example the 1,9th part of a 700MB

CD. For the example of mp3 music streams at 128kBit set this to 16220160.

C3SURF_TRAFFIC_MINUTES `C3SURF_TRAFFIC_BYTES='16'`

Value range: natural numbers

Specifies the time in minutes that elapses between two data volume measurements. If, after the elapsed time an excess is found here, the responsible party is first temporarily stored. If again found to be exceeded during the next measurement, it is automatically logged out and blocked (for `C3SURF_TRAFFIC_BLOCKTIME` (Page 19) minutes). If no exceeding is detected in the second measurement, the temporary storage is deleted.

For the mp3 example set '15' here.

C3SURF_TRAFFIC_BLOCKTIME `C3SURF_TRAFFIC_BLOCKTIME='60'`

Value range: natural numbers

Specifies the time in minutes for that access is blocked after exceeding the traffic limits.

1.10. General Informations

1.11. fli4l Web Interface

Rights: c3surf:view, admin

- view: Show the entry in Admin menu
- admin: To use functions in the web interface.

  Httpd users with right "all" have all rights here too.
- OPT C3SURF can be found in the Web interface at "Opt" -> "c3Surf".

1.12. Operation

With c3surf single hosts or complete nets may be defined that are blocked after system boot then. By an informal registration via the web interface users can unlock circuits for a defined time span.

If the option LOGINUSR is activated, only persons with a valid user name and password will be allowed to log in.

In the Admin interface of the router users or MAC addesses may be displayed, logged out or blocked, either permanently or time based. These locks are only vaild for the registration with c3Surf and are managed there. The lock is meaningless if the PC in question gains access to the router via another interface.

The registration is accomplished with first-, lastname and E-Mail address or via user/password. After a defined time the access is blocked again and has to be reactivated by a new login.

The registration page may also be locked for the users (see FreeSurf resp. LoginUsr in the OPT menue of the Web interface).

All this operations are part of the Admin menu of the Web interface.

If a defined host should be unblocked permanently this may be done in the Web interface (see the ARP lists or DHCP leases).

All usage can be restircted by Quotas. This restricts use time and by the parameters "-TIME", "-BLOCKTIME" and "-COUNTER" a variety of configuration options are available.

Examples:

Time	Blocktime	Counter	Quota (`C3SURF_QUOTA='yes'`)
60	-1	0	60 Min use time, No lock after timeout, With every registration the time is running (parking meter principle)
60	240	0	60 Min use time, after timeout locked for 240 mins., With every registration the time is running (parking meter principle= Money in, no chance of interception)
60	0	-1	60 Min use time, after timeout locked until 00:00 o'clock, any number of logins and logouts possible (no parking meter principle)
60	-1	1	60 Min use time, no lock after timeout, time may be intercepted once
60	-1	-1	60 Min use time, no lock after timeout, as many interceptions as you like
600	10080	-2	10 hours within a week with as many interceptions as you like
0	-1	0	Endless use time with each registration, no lock after timeout

1.13. Name Resolution - DNS

Important: fli4l has to be entered as the DNS-Server on all clients and must be able to perform name resolution. This either

- **needs a "Forward" to the DNS server of the net or**
- **fli4l itself is the DNS server and may establish connections if needed.**

Otherwise problems arise to redirect to the registration page automatically.

But it may also be accessed manually by specifying its URL in the browser.

1.14. Miscellaneous

1.14.1. Warning

Important: *Without* `OPT_LOGINUSR='yes'` *(Page 12) any person with an IP address assigned to their computer by the router (eg from an open Wi-Fi), has free access to the Internet and unblocked services on the router. c3Surf is helpful for blocking services, but is no substitute for a proper configuration of the firewall in base.txt.*

1.14.2. Recommendation

Important: *The router should contain a recovery version build. With an improper configuration you may lock yourself out completely.*

1.14.3. Errors

Error descriptions containing config informations may be posted on the fli4l newsgroups http://www.fli4l.de/hilfe/newsgruppen-forum/.

1.14.4. License

This software is licensed under the terms of the GNU General Public License published in version 2 or following. According to it, this software is free for users, developers and companies. It is good style, to mention the original developers when further using this piece of software. This is especially true for public domain works.

1.14.5. Literature

If you like to open your net to others you should concern the legal situation.

A CC licensed work (in german) can be found at:
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. Appendix For Package C3SURF

Opt and Docs:	07. Januar 2008	Frank Saurbier	mailto:c3surf@arcor.de
Tex-Docs:	01. April 2009	Helmut Backhaus	mailto:helmut.backhaus@gmx.de
Handover:	01. Mai 2010	fli4l-Team	mailto:team@fli4l.de

A.1. Hints Concerning Other Opts

A.1.1. cpmvrmlog Config

Example For The C3SURF Log Directory, With mini_httpd Restart

```
# archive C3SURF log dir
# once in a month on the 1.st at 01:30
# keep a maximum of 12 archives
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. Allow Samba Without Login

Use opt_usercmd with the following entries.

```
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
```

By adding the option `-d IPsambaHOST` the rules may be enhanced to reflect the target PC.

Samba ports will pass the Forward-Chain and are not blocked by C3SURF. If the Forward-Chain denies samba forwards these entries will not change anything stated there.

The settings in base.txt supersede these settings.

A.1.3. Migration From Previous Versions

- Migration to Version 2.3.1 (from 2.3.0)
  - New variables, only optional. The new range is marked in config.txt like this
  - "# + new 2.3.1 + begin ———————— delete this line".
  - The voucher format has changed, old voucher may still be used, but will not be recognized when generating new ones. To tidy up, delete all vouchers and generate new ones.
- Migration to Version 2.3.0 (from 2.2.2)
  - If not using vouchers no changes are needed.
  - New variables for OPT_C3SURF_VOUCHER, if vouchers should be used.
  - The new range is marked in config.txt like this
  - "# + new 2.3.0 + begin ———————— delete this line".
- Migration to Version 2.2.2 (from 2.2.1)
  - New variables. The new range is marked in config.txt like this
  - "# + new 2.2.2 + begin ———————— delete this line".
  - C3SURF_CONTROL_SQUID: optional to control squid, temporary as squid does not follow fli4l's conventions.
  - Variables for overwriting Quota-Defaults with LOGINUSR_ACCOUNT are now optional
- Migration to Version 2.2.1 (from 2.2.0)
  - New variables. The new range is marked in config.txt like this
  - "# + new 2.2.1 + begin ———————— delete this line".
  - C3SURF_WORKON_TMP: recommendation for harddisk idle mode 'yes' else 'no'

also with FLASH.

- C3SURF_SAVE_QUOTA: recommendation 'yes'.

- Migration to Version 2.2.0 (from 2.1.0)
  - New variable "C3SURF_CHECK_ARP" in config (recommendation: 'yes'). It is marked in config.txt like this
  - "# + new 2.2.0 + begin ———————— delete this line".

- Migration to Version 2.1.0 (from earlier versions)
  - New variables. The new range is marked in config.txt like this
  - "# + new 2.1.0 + begin ———————— delete this line".
  - The MAC-Blackliste (if existing) has to copied to the directory "C3SURF_PERSISTENT_PATH" manually.
  - The format of c3surf_login.log has been expanded by a row. Save old logs and delete them in C3SURF_LOG_PATH.

Index