Package HTTPD - Webserver For Status-Display Version 3.10.18

Frank Meyer
email: frank@fli4l.de

the fli4l-Team
email: team@fli4l.de

September 15, 2019

Contents

1. Documentation For Package HTTPD

1.1. HTTPD - Webserver For Status-Display

1.1.1. OPT_HTTPD - Mini-Webserver As Status-Display

The webserver can be used to display or change the status of fli4l routers (IMONC can be used too). The status monitor can be activated by setting `OPT_HTTPD='yes'`.

If you are using the default configuration set your browser to one of the following addresses:

```
http://fli4l/
http://fli4l.domain.lan/
http://192.168.6.1/
```

If you configured fli4l to use another name and/or domain these have to be used. If the webserver is set to listen on another port than the default one specify it like this:

```
http://fli4l:81/
```

As of version 2.1.12 a login page will be displayed which is not protected by a password. Protected pages are in the subdirectory admin, for example:

```
http://fli4l.domain.lan/admin/
```

The web server can be configured by setting the following variables:

HTTPD_GUI_LANG This specifies the language in which the web interface is shown. If set to 'auto' the language setting is taken from the variable `LOCALE` in base.txt.

HTTPD_LISTENIP The web server usually binds to a so-called wildcard address in order to be accessed on any router interface. Set the web server with this parameter to only bind to one IP address. The corresponding IP address is given here: `IP_NET_x_IPADDR`. Normally this parameter is left blank, so the default (Accessible on any interface IP) is used.

This parameter is used to bind the httpd to only one IP so that other instances can bind to other IPs on the router. It can not be used to limit access to the web interface of the router. This would need additional configuring of the packet filter, too.

It is also possible to specify multiple IP addresses here (separated by spaces).

HTTPD_PORT Set this value if the web server should run on another port than 80. This is usually not recommended, since then it must be accessed through the browser by adding the port number. Example http://fli4l:81/.

HTTPD_PORTFW If setting this variable to 'yes' you can change port forwarding via the web interface. Rules can be erased and/or added. Changes take effect immediately and only apply during router runtime. If the router is restarted, the changes are gone. The default setting is 'yes'.

HTTPD_ARPING The web server displays the online/offline state of the hosts listed in HOST_x. To achieve this it uses the *"Arp-Cache"*, a cache that buffers the addresses of the local hosts. If a host does not communicate with the router for longer its address will disappear from the *"Arp-Cache"* and it appears to be offline. If you want to keep the *"Arp-Cache"* up-to-date (keep the online hosts that are not communicating with the router in it) set HTTPD_ARPING='yes'?.

HTTPD_ARPING_IGNORE_N Sets the number of entries to be ignored when arping

HTTPD_ARPING_IGNORE_x IP-adress or name of the hosts not to be included in ARPING-tests. This may be useful for battery based hosts consuming too much power by regular network queries (i.e. laptops or cell phones in WLAN).

1.1.2. User Management

The webserver provides a sophisticated user management:

HTTPD_USER_N Specify the number of users. If set to 0 user management will be switched off completely so everybody can access the web server.

HTTPD_USER_x_USERNAME HTTPD_USER_x_PASSWORD HTTPD_USER_x_RIGHTS enter username and password for each user here. On top specify for each user which functions of the the web server should be accessible to him. Functions are controlled via the variable HTTPD_RIGHTS_x. In the simplest case it is 'all', which means that the corresponding user is allowed to access everything. The variable has the following structure:

```
'Range1: right1,right2,... Range2:...'
```

Instead of adding all rights for a certain range the word "all" can be used. This means that the user has all rights in this range. The following ranges and rights exist:

Range "status" Everything in menu 'Status'.

- **view** User can access all menu items.
- **dial** User can dial and hang up connections.
- **boot** User can reboot and shut down the router.
- **link** User can switch channel bundeling.
- **circuit** User can switch circuits.
- **dialmode** User can switch dialmodes (Auto, Manual, Off).
- **conntrack** User can view currently active connections.
- **dyndns** User can view logfiles of package DYNDNS (Page **??**).

Range "logs" Everything concerning log files (connections, calls, syslog)

- **view** User can view logfiles.
- **reset** User can delete logfiles.

Range "support" Everything of use for getting help (Newsgroups a.s.o.).

- **view** User can access links to documentation, fli4l-website, a.s.o.

systeminfo User can query detailed informations about configuration and actual status of the router (i.e.: firewall).

Some examples:

HTTPD_USER_1_RIGHTS='all' Allow a user to access everything in the webserver!

HTTPD_USER_2_RIGHTS='status:view logs:view support:all' User can view everything but can't change settings.

HTTPD_USER_3_RIGHTS='status:view,dial,link' User can view the status of internet connections, dial and switch channel bundeling.

HTTPD_USER_4_RIGHTS='status:all' User can do everything concerning internet connections and reboot/shutdown. He is not allowed to view or delete logfiles (nor timetables).

1.1.3. OPT_OAC - Online Access Control

OPT_OAC (optional)

Activates 'Online Access Control'. By using this internet access of each host configured in package dns_dhcp (Page **??**) can be controlled selectively.

A console tool is available too, providing an interface to other packages like EasyCron:

/usr/local/bin/oac.sh

Options will be shown when executed on a console.

OAC_WANDEVICE (optional)

Restricts the online access control to connections on this network device (i.e. 'Pppoe').

OAC_INPUT (optional)

Provides protection against circumvention via proxy.

OAC_INPUT='default' blocks default ports for Privoxy, Squid, Tor, SS5, Transproxy.

OAC_INPUT='tcp:8080 tcp:3128' blocks TCP Port 8080 and 3128. This is a space separated list of ports to be blocked and their respective protocol (udp, tcp). Omitting protocols blocks both udp and tcp.

Omitting this variable or setting it to `'no'` deactivates the function.

OAC_ALL_INVISIBLE (optional)

Turns off overview if at least one group exists. If no groups exist the variable is without effect.

OAC_LIMITS (optional)

List of available time limits separated by spaces. Limits are set in minutes. This allows time period based blocking or access definition.

Default: '30 60 90 120 180 360 540'

OAC_MODE (optional)

Possible values: `'DROP'` or `'REJECT'` (default)

OAC_GROUP_N (optional)

Number of client groups. Used for clarity but also allows to block or allow access for a whole group at once over the web interface.

OAC_GROUP_x_NAME (optional)

Name of the group - this name will be displayed in the web interface and may be used in console script 'oac.sh'.

OAC_GROUP_x_BOOTBLOCK (optional)

If set to `'yes'` all clients of the group are blocked at boot. Useful if PCs should be blocked in general.

OAC_GROUP_x_INVISIBLE (optional)

Marks the group as invisible. Useful to block a PC in general which should not be visible in the web interface. The console script oac.sh is not affected by this (for use in easycron).

OAC_GROUP_x_CLIENT_N (optional)

Number of clients in the group.

OAC_GROUP_x_CLIENT_x (optional)

Name of the client as defined in `HOST_x_NAME` in package dns_dhcp (Page **??**).

OAC_BLOCK_UNKNOWN_IF_x (optional)

List of interfaces defined in base.txt allowing internet access only to hosts defined in dns_dhcp.txt. Hosts not defined are blocked in general.

A. Appendix For Package HTTPD

A.1. HTTPD

A.1.1. Additional Settings

These variables are not present in the configuration and thus have to be added to it when needed.

HTTPD_USER By using this option the web server can be run with the rights of another user than „root". This is useful especially if the webserver should display other pages than the admin interface. **Scripts that need access to configuration files possibly won't run as expected then. Standard scripts will run with any user provided.**

A.1.2. Remarks

If TELMOND is installed the telephone numbers of callers will be displayed on the pages 'status' and 'calls'. Names can be assigned via entries in the file opt/etc/phonebook. This file has the same format as IMONC's telephone number file. Phonebooks may be exchanged between IMONC and the router. The format of each row is "Phone number=Name[,WAV-file]" WAV files will only be used by IMONC and are ignored by the web server.

The complete web interface has been converted to frameless design using css as of version 2.1.12. Really old browsers may have problems displaying this. The advantage is that the look of the pages can be changed almost completely simply by editing the css files (mainly /opt/srv/www/css/main.css).

The webserver package was devloped by Thorsten Pohlmann (email: pohlmann@tetronik.com) and is maintained by Tobias Gruetzmacher (email: fli4l@portfolio16.de) at the moment. The new design (as of version 2.1.12) was realized by Helmut Hummel (email: hh@fli4l.de).

List of Figures

List of Tables

Index