

WIRELESS ACCESS POINT



CONFIGURATION MANUAL

Version: 1.0 for firmware V20.48.00 | Date: 14.04.2021

Contents

1	IMPO	RTANT INFORMATION	1
	1.1	Revision	1
	1.2	Disclaimer	1
		1.2.1 Copyright	1
		1.2.2 GPL Statement for CyBox Software	1
		1.2.2.1 Disclaimer of Warrenty	2
		1.2.2.2 Limitation of Liability	2
		1.2.3 Regulatory Limits for Changes in Country and Transmit Power Settings	2
	1.3	Known Issues	2
2	ABOU	T THIS DOCUMENT	3
	2.1	Information about Formatting	3
3	ABOU	T THE CyBox AP 3	3
4	HOW	TO ACCESS THE CyBox AP 3	4
	4.1	IP Addresses of the CyBox AP 3	4
	4.2	Getting to the Web Interface	5
5	QUIC	K START GUIDE	6
	5.1	Change Password	6
	5.2	Change LAN IP address (Quick Guide)	6
		5.2.1 Disabling IPv6	7
	5.3	Example: Local Access Point	8
		5.3.1 System Settings	8
		5.3.2 Prepare WLAN Radio Interface	8
		5.3.3 Connect radio0 to the Network	9
		5.3.4 Connecting to WAN	10
	5.4	Example: Connecting three VLANs to a server	10
		5.4.1 Create the Management VLAN	11
		5.4.2 Add two unmanaged VLANs	11
		5.4.3 Configure and Enable the radio(s)	12
		5.4.4 Attach the "Clients" VLAN to radio0	12
		5.4.5 Attach the "Staff" VLAN to radio0	13
		5.4.6 Check Configuration	13
		5.4.7 Disable Unneeded Default Address	14
	5.5	Example: Client Isolation within the Access Point	14
		5.5.1 Isolate the Radio Clients	14

5.5.2 Restrict Access to Local Ports to Specified Interfaces	14
6 THE WEB INTERFACE	15
6.1 Network	15
6.1.1 Interfaces	15
6.1.1.1 DHCP Server per Interface	15
6.1.1.2 Bridges	15
6.1.1.3 VLAN	16
6.1.2 WLAN	17
6.1.2.1 Channel, Wireless mode, HT mode, Power settings	18
6.1.2.2 Radio Band Configuration for Models with Antenna Combiner	19
6.1.2.3 JJPlus Radio Card Band Configuration	19
6.1.2.4 ESSID, WDS Mode, Client separation	20
6.1.2.5 Encryption	20
6.1.2.6 Hotspot 2.0	22
6.1.2.7 WLAN Clients test	22
6.1.2.8 Multi-AP Client Isolation	22
6.1.2.9 Connection Check	23
6.1.2.10 Access Point Scanning Service (Wireless Monitoring)	24
6.1.2.11 Client Counting Service	26
6.1.2.12 Rogue Access Point Detection Service	29
6.1.3 Multi-WAN Manager (MWAN3)	30
6.1.3.1 Capabilities	32
6.1.3.2 MWAN Test	32
6.1.3.2.1 Gateway	32
6.1.3.3 MWAN Status	33
6.1.3.4 MWAN Modem Interface Configuration	34
6.1.3.5 MWAN Members Configuration	36
6.1.3.6 MWAN Policies Configuration	37
6.1.3.7 MWAN Rules Configuration	38
6.1.3.8 MWAN Notification Configuration	38
6.1.4 MultiPath TCP / Link Aggregation	39
6.1.4.1 OpenMPTCProuter versus MWAN3	40
6.1.4.2 OpenMPTCProuter/MWAN3 selection	41
6.1.4.3 VPS Configuration	41
6.1.4.3.1 Recommendations	41
6.1.4.3.2 Install / setup VPS tools	41

ELTEC systems

6.1.4.3.3 Generated keys	42
6.1.4.3.4 Choosing a VPN Technology	42
6.1.4.4 OpenMPTCProuter configuration example	42
6.1.4.4.1 Setup DHCP	42
6.1.4.4.2 Remove / Disable unused default interfaces	43
6.1.4.4.3 Setup LTE Modems	43
6.1.4.4.4 Setup MPTCP	45
6.1.4.4.5 Setup VPS access	46
6.1.4.4.6 Speed test / IP	48
6.1.5 LACP / Bonding	49
6.1.5.1 LACP configuration example	49
6.1.5.1.1 Create LACP interface	50
6.1.5.1.2 Setup IP / Netmask	50
6.1.5.1.3 Setup bonding Policy / add slave Interfaces	50
6.1.5.1.4 Setup Firewall	51
6.1.5.1.5 Check interface Status	52
6.1.5.2 LACP testing example	53
6.1.5.2.1 Test Setup	53
6.1.5.2.2 Test bonding bandwidth improvement	54
6.1.5.2.3 Test bonding reliability improvement	54
6.1.6 Global DHCP and DNS Settings	54
6.1.7 Firewall	55
6.1.8 OpenVPN	56
6.1.8.1 Configuration file generation on Windows	56
6.1.8.2 VPN interface setup – 3 methods	56
6.1.8.2.1 Copy Ready-to-use configuration with SCP	56
6.1.8.2.2 Upload configuration, certs, key-files with web interface	57
6.1.8.2.3 Manual configuration with web interface	58
6.1.8.3 VPN host configuration (on console)	58
6.1.9 ICCP	60
6.1.9.1 Coupling Concept	60
6.1.9.2 SSID Usage	61
6.1.9.3 WLAN Encryption	61
6.1.9.4 Configurable Parameters	61
6.1.9.5 Configuration Hint Web Interface	63
6.1.9.6 VLAN over Wireless ICCP	64

systems

	6.1.9.6.1 Features and Restrictions	64
	6.1.9.6.2 Examples	64
	6.1.10 QoS	68
6.2	GPS	68
	6.2.1 GPS activation	68
	6.2.2 GPS status	69
	6.2.3 SNMP for GPS	70
6.3	System	71
	6.3.1 Configuration Backups	71
	6.3.2 Firmware Upgrade	71
	6.3.3 Reboot	72
	6.3.4 Reset Button	72
	6.3.5 Emergency Mode	72
7 SNMP		74
7.1	SNMP Protocol Support	74
7.2	SNMP V3 Protocol Support	74
	7.2.1 SNMP V3 Protocol Examples	75
7.3	SNMP Basic Functions	76
7.4	SNMP Read and Write Authorizations	76
7.5	SNMP Commands	77
7.6	SNMP Read (snmpwalk and snmpget)	78
	7.6.1 Reading System Information	78
	7.6.2 Reading SNMP Object Information	78
	7.6.2.1 Readout current Network Device Order	79
	7.6.2.2 Readout SSID / WIFI Interface Order	79
	7.6.2.3 Readout Network Device to SSID Assignment	80
7.7	SNMP Write (snmpset)	81
	7.7.1 Direct command	81
	7.7.1.1 Reboot	81
	7.7.2 Edit configuration using Object Identifier (OID)	81
	7.7.2.1 Set a new IP address	81
	7.7.2.2 Set a new SSID	81
	7.7.2.3 Set a new Macfilter	82
	7.7.3 Edit configuration parameters, create new fields and delete items	82
	7.7.3.1 Set new Hostname	83
	7.7.3.2 Creating a system configuration description text	83

7.7.3.3 Delete system configuration description text	84
7.8 SNMP Applications	84
7.8.1 SNMP Support for GPS	84
7.8.2 SNMP Support for Second GPS Source	86
8 THE FLYING CONTROLLER MECHANISM	87
9 IPSecVPN / StrongSwan	87
9.1 IPSec Customized Configuration	87
9.2 IPSec default configuration	88
9.3 IPSec Secret configuration	89
9.4 IPSec Tunnel / Transport Connection	90
9.5 IPSec Crypto Proposal configuration	91
9.6 IPSec Firewall Custom Rules	92
9.7 IPSec Service Start	93
10 SSH / SERIAL CONSOLE	94
10.1 UCI Configuration	95
10.1.1 UCI configuration files	95
10.1.2 UCI Example	95
10.2 Other commands	96
11 SYSTEM MAINTENANCE	96
11.1 Remote Firmware Upgrade	96
11.1.1 Remote Firmware Upgrade without Config Change	96
11.1.2 Remote Firmware Upgrade with New Config	96
11.2 USB Possibilities	98
11.3 Status LED Blink Codes	99
12 APPENDIX: GPL LICENSE	100
13 APPENDIX: SNMP OID OVERVIEW	110
14 APPENDIX: DEFAULT FACTORY SETTINGS	112

V

systems

1 IMPORTANT INFORMATION

1.1 Revision

Internal version: ff6db28

Revision	Changes	Date
1.0	Initial version for this firmware	14.04.2021

1.2 Disclaimer

1.2.1 Copyright

© 2018-2021 ELTEC Elektronik AG. The information, data, and figures in this document including respective references have been verified and found to be legitimate. In particular in the event of error they may, therefore, be changed at any time without prior notice. The complete risk inherent in the utilization of this document or in the results of its utilization shall be with the user; to this end, ELTEC Elektronik AG shall not accept any liability. Regardless of the applicability of respective copyrights, no portion of this document shall be copied, forwarded or stored in a data reception system or entered into such systems without the express prior written consent of ELTEC Elektronik AG, regardless of how such acts are performed and what system is used (electronic, mechanic, photocopying, recording, etc.). All product and company names are registered trademarks of the respective companies.

Our General Business, Delivery, Offer, and Payment Terms and Conditions shall otherwise apply.

1.2.2 GPL Statement for CyBox Software

This software product contains software covered by the GNU GPL (see below in this document), it may in addition contain other parts covered by other licenses (such as LGPL). A list of all modules and their licenses ("FOSS" list) is available on request (see link below). The source code of all GPL-covered modules can also be requested by owners of the CyBox AP 3-W/LTE (see link below).

For the GPL-covered parts this license is valid:

Copyright (c) 2014-2021, ELTEC Elektronik AG This program is free software: you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation, either version 3 of the License, or (at your option) any later version. This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details. You should have received a copy of the GNU General Public License along with this program. If not, see <https://www.gnu.org/licenses/>.

FOSS and sources are not included in the binary distribution in the products and in the product documentation due to space limitations.

Use this link to request FOSS and sources, please send in your request by mail (handling fees for sources may apply):

ELTEC Elektronik AG

Galileo-Galilei-Str. 11

55129 Mainz

Germany

1.2.2.1 Disclaimer of Warrenty

There is no warranty for the program, to the extent permitted by applicable law. except when otherwise stated in writing the copyright holders and/or other parties provide the program "as is" without warranty of any kind, either expressed or implied, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. The entire risk as to the quality and performance of the program is with you. Should the program prove defective, you assume the cost of all necessary servicing, repair or correction.

1.2.2.2 Limitation of Liability

In no event unless required by applicable law or agreed to in writhing will any copyright holder, or any other party who modifies and/or conveys the program as permitted above, be liable to you for damages, including any general, special, incidental or consequential damages arising out of the use or inability to use the program (including but not limited to loss of data or data being rendered inaccurate or losses sustained by you or third parties or a failure of the program to operate with any other programs), even if such holder or other party has been advised of the possibility of such damages.

You should have received the following text in an "About" box (see Tab "System") together with the product. Here it is replicated for reference:

This software product contains software covered by the GNU GPL license. A list of all modules and their licenses ("FOSS" list) is available on request, as is the source code of all GPL-covered modules. For details and GPL text, see the Software Configuration Manual, available on <https://www.eltec.com>. In case of problems use the mail (street) address below. Request FOSS and sources with a mail to: ELTEC Elektronik AG Galileo-Galilei-Str. 11 55129 Mainz Germany

1.2.3 Regulatory Limits for Changes in Country and Transmit Power Settings

Make sure that only persons with proper knowledge also in regulatory matters have access to the access point's configuration settings. They must be aware of the consequences of an improper setting of country and transmit power (there may be additional settings). To do so, the standard configuration password must be changed before the access point is deployed. This new password must be given to knowledgeable and responsible persons only.

One example of a regulation affecting country selection is that in Germany, as of October 2016, the frequencies in the range 5150 MHz - 5350 MHz must be used in closed rooms and similar environments only. For more information please see www.bundesnetzagentur.de.

1.3 Known Issues

• When operating WLAN in 11ac mode, the transmit data rate is erroneously wrongly reported as 6 Mbit/s.

2 ABOUT THIS DOCUMENT

This configuration manual is intended for system developers and integrators. It is not intended for end users. It describes the firmware functions of the access point/router/gateway product family and provides information for special applications and configurations of the product.

This manual is intended to guide through the configuration process of an Access Point/Router/Gateway (the names of which are used interchangeably for this manual) for use in a train or bus. We tried to cover the main aspects of this task, including

- Backup and restore of configurations
- Install new firmware versions
- Handling of IP addresses, DHCP, VLAN, VPN, firewall
- Configuration of WiFi and LTE
- MWAN configuration for multiple WAN connection
- ELTEC's train coupling, wireless backbone protocol ICCP
- Remote administration via SNMP
- Scripting and UCI.

Not covered is a complete list of all functions and of all configuration elements in detail.

Information about mechanical and electrical installation of the access points is available in a separate product-specific installation manual which can be downloaded from the Download Center at www.eltec.com.

2.1 Information about Formatting

In the following sections, text formatted like this refers to titles, tabs, boxes, menu names, group names, keys, and other descriptive text on the web-based configuration user-interface ("LuCI"). They are grouped by " \rightarrow ".

This markup is used for all navigation elements needed to access settings, independent from the elements used to click on them or just for visual grouping.

A typewriter font is used for text typed in.

3 ABOUT THE CyBox AP 3

The CyBox AP 3 is a member of the CyBox family of robust wireless railway access points. It is particularly designed to meet the requirements of rolling stock applications. It offers stable, secure, and high bandwidth connections between the local Ethernet and wireless clients. With the assistance of the access point, multiple mobile Wi-Fi-compatible devices in a passenger train or subway have the possibility to communicate with the Internet or access local data, for example.

The CyBox AP 3 firmware provides a convenient management interface via a web service. Besides global setup parameters the open source software allows the configuration of the radio interfaces, such as channel selection, SSID, encryption keys, and firewall setup. The access point and router configurations as well as the management firmware can be updated remotely.

The firmware of the device is based upon Linux and OpenWRT/LEDE. For Open Source information see the preface.

4 HOW TO ACCESS THE CyBox AP 3

The CyBox AP 3 can be configured in several ways:

- 1. The graphical web interface
- 2. The command line interface via a SSH or serial connection, see 10 SSH / SERIAL CONSOLE
- 3. Using an USB stick (to update the firmware or apply a prepared configuration, see 11.2 USB Possibilities)
- 4. Using SNMP (see 7 SNMP)

4.1 IP Addresses of the CyBox AP 3

By default, the CyBox AP 3 is accessible through the following IP addresses (see figure The page Network \rightarrow Interfaces (default settings)):

- 192.168.100.1 (LAN)
- An address obtained using DHCP (if possible LAN_DHCP)
- An address derived from the serial number (LAN_ALIAS)
- An address derived from the MAC of the first Ethernet port (LAN_MAC)

The LAN_ALIAS address is derived from the serial number (which is printed on the type plate) as follows (Example Serial Number: EL303289):

- 1. Strip non-digits: 303289
- 2. Print as six-digit hex value: 0x04A0B9
- 3. Use the upper 8 bits for x, the middle for y and the lower for z: x=0x04 y=0xA0 z=0xB9
- 4. Convert x,y,z to decimal: x=4 y=160 z=185
- 5. The LAN_ALIAS address is 10.4.160.185

In a similar manner, the LAN_MAC address is derived from the MAC address of the first Ethernet interface, which is printed on the type plate (example MAC 00:00:5B:04:AE:03):

- 1. Take the last three bytes: 04:AE:03
- 2. Use the upper 8 bits for x, the middle for y and the lower for z: x=0x04 y=0xAE z=0x03
- 3. Convert x,y,z to decimal: x=4 y=174 z=3
- 4. The LAN_MAC address is 10.4.174.4

You can delete unneeded network interfaces by clicking on the red "Delete" button in the web interface.

systems

Status	LAN LAN_ALIAS	AN_DHCP LAN_MAC MODEM	S1 MODEM_S2		_
System	Interfaces		<u> </u>		
VPN		Protocol: Static address			
Services	LAN_ALIAS	Uptime: 0h 3m 42s MAC: 00:00:5B:04:AE:03			
Network	eth0	RX: 61.06 KB (585 Pkts.) TX: 364.48 KB (727 Pkts.)	Restart	Stop Edit	Delete
Interfaces	1	IPv4: 10.4.160.185/8			
Wireless	LAN_DHCP	Protocol: DHCP client MAC: 00:00:5B:04:AE:03	Restart	Stop Edit	Delete
DHCP and DNS	eth0	RX: 61.06 KB (585 Pkts.) TX: 364.48 KB (727 Pkts.)		Con	
Hostnames		Protocol: Static address			
Static Routes	LAN_MAC	Uptime: 0h 3m 42s MAC: 00:00:5B:04:AE:03	Destart)	Stop Edit	Delete
Diagnostics	eth0	RX: 61.06 KB (585 Pkts.) TX: 364.48 KB (727 Pkts.)	Restart	Stop Edit	Delete
Firewall		IPv4: 10.4.174.3/8			
Client Isolation		Protocol: Static address Uptime: 0h 3m 42s			
Connection Check	LAN	MAC: 00:00:5B:04:AE:03		a . a .	
QoS	eth0	RX: 61.06 KB (585 Pkts.) TX: 364.48 KB (727 Pkts.)	Restart	Stop Edit	Delete
Configure Diagnostics		IPv4: 192.168.100.1/24 IPv6: fdb9:bebd:8f2::1/60			
Load Balancing		Protocol: ModemManager			
Statistics	MODEM_S1	RX: 0 B (0 Pkts.) TX: 0 B (0 Pkts.)	Restart	onnect Edit	Delete
	wwan_S1_0	Information: Not started on boot Error: Unknown error (sim-missin		Curt	
Logout		Protocol: ModemManager	9/		
	MODEM_S2	RX: 0 B (0 Pkts.) TX: 0 B (0 Pkts.)	Restart	onnect Edit	Delete
	wwan_S2_0	Information: Not started on boot Error: Unknown error (sim-missin		onnect Luit	Detete
	Add new interface				
	Global network op	tions			
	IPv6 ULA-Prefix	fdb9:t	oebd:08f2::/48		
	1			Save & Apply	Save Reset

The page Network \rightarrow Interfaces (default settings)

4.2 Getting to the Web Interface

Before accessing the web interface, your computer must be connected to the Ethernet port LAN 1, and it must be configured to use the same subnet as the CyBox AP 3.

The web interface is accessible using HTTPS on the IP addresses listed in 4.1 IP Addresses of the CyBox AP 3 (default: https://192.168.100.1/ in the subnet 192.168.100.0/24). It uses a self-signed SSL certificate. Your browser should warn you about that. You can either accept the certificate or fall back to HTTP: http://192.168.100.1/.

On the login web page, use username root and password root. Of course, you should 5.1 Change Password as soon as possible.

Once connected, you can navigate through the different tabs to start configuration. A few rules apply:

- To apply and also save your configuration, click on the button Save & Apply on the bottom-right corner of most pages. Not clicking on this button will discard your modifications.
- Saved configurations will be kept after a reboot.
- If IP addresses are changed, the Access Point must be addressed under the new URL in the browser.

5 QUICK START GUIDE

This chapter describes the steps to configure standard access point operation. The device must be electrically connected (see installation manual). Factory default settings are used.

This chapter shows some common use-cases and an exemplary implementation for each.

When the CyBox AP 3 configuration requires deep changes, e.g. for a new use-case, there is some risk that previous (maybe meanwhile forgotten) settings get into conflict with the new configuration. Thus it is recommended to start the configuration from factory default settings. Pressing the hardware reset switch for more than 5 seconds will restore the factory settings.

The web interface provides the same function: $System \rightarrow Backup / Flash Firmware \rightarrow Perform reset.$

For all below configuration examples, the following initial situation is assumed:

- CyBox AP 3 is running
- CyBox AP 3 has been reset to factory defaults, the IP address is 192.168.100.1
- Default Root-User password: 'root'
- Operator workstation and CyBox AP 3 are connected via Ethernet
- Workstation browser is logged-in to the CyBox AP 3 web interface
- Operator is additionally logged in to CyBox AP 3 via SSH (if available, a serial console terminal would be preferable).

In the following examples [square brackets] are used to indicate actions not requiring operator interaction because they happen automatically or have already been done (mentioning them here might be useful for checking configuration is on the right way).

5.1 Change Password

The password should be changed first to avoid legal consequences as described in the preface. The default user/password is'root'/'root'. To change it, go to $System \rightarrow Administration$, type new password and click Save.

Status	Router Password SSH Access SSH-Keys	
System	Router Password	
System	Changes the administrator password for accessing the	device
Administration	Password	*
Startup		
Scheduled Tasks	Confirmation	*
Mount Points		Password strength:
Backup / Flash Firmware	5	Save
Custom Commands		Save

Change Password

5.2 Change LAN IP address (Quick Guide)

The factory default IP address 192.168.100.1 must be changed to meet your network topology. Open Network → Interfaces and click the Edit button of the LAN interface. Modify the IP address (IPv4 address field), or change the Protocol field to DHCP client, then click on Save & Apply. To regain access to the web interface, you must type the new IP address in your browser.

systems

CYBOX AP 3

Status St	Physical Settings Firewall Settings DHCP Server Device: eth0 Uptime: 1h 27m 45s MAC: 00:00:58:03:85:79 PX: 1.49 MB (8494 Pkts.) TX: 2.14 MB (3808 Pkts.)
Protocol Si Bring up on boot Si IPv4 address 15 IPv4 netmask 25 IPv4 gateway I IPv4 broadcast 15 Use custom DNS servers I IPv6 assignment length 6 Q IPv6 assignment hint 0 Q	Uptime: 1h 27m 45s MAC: 00:00:5B:03:B5:79 RX: 1.49 MB (8494 Pkts.)
Bring up on boot IPv4 address IPv4 address 15 IPv4 netmask 25 IPv4 gateway IPv4 broadcast IPv4 broadcast 15 Use custom DNS servers IPv6 assignment length IPv6 assignment hint 0	IPv4: 192.168.100.1/24 IPv6: fd96:db0e:c0f1::1/60
IPv4 address 19 IPv4 netmask 22 IPv4 gateway 19 IPv4 broadcast 19 Use custom DNS servers 19 IPv6 assignment length 60 IPv6 assignment hint 10	atic address 🔹
IPv4 netmask 25 IPv4 gateway 1 IPv4 broadcast 15 Use custom DNS servers 1 IPv6 assignment length 60 IPv6 assignment hint 0	
IPv4 gateway IPv4 broadcast IS Use custom DNS servers IPv6 assignment length @ IPv6 assignment hint @	2.168.100.1
IPv4 broadcast [15] Use custom DNS servers IPv6 assignment length @ IPv6 assignment hint 0 @	5.255.255.0
Use custom DNS servers IPv6 assignment length IPv6 assignment hint IPv6 assignment hint IPv6 assignment hint IIPv6 assignment hint I	
IPv6 assignment length 60 IPv6 assignment hint 0	2.168.100.255
IPv6 assignment hint	+
2	Assign a part of given length of every public IPv6- prefix to this interface
	Assign prefix parts using this hexadecimal subprefix ID for this interface.
IPv6 suffix ::1	Optional. Allowed values: 'eui64', 'random', fixed value like '::1' or '::1:2'. When IPv6 prefix (like 'a:b:c:d::') is received from a delegating server, use the suffix (like '::1') to form the IPv6 address ('a:b:c:d:') for the interface.

LAN Configuration Example

5.2.1 Disabling IPv6

The custom helper script under System \rightarrow Custom Commands \rightarrow Dashboard will modify the network / firewall configuration to disable all IPv6 network traffic. Normally all network interfaces have an automatic IPv6 address applied. If your environment has no need for IPv6 network traffic, you should use this script in early configuration steps, to remove every IPv6 address setup form network interfaces and to remove IPv6 firewall rules. Note that the Run button has to be executed twice. The first time is only for user information. The configuration modification is permanent.

Status	Dashboard Configure		
System	Custom Commands		
System			
Administration	System Information	System IPv6 Disable	Wireless Info
Startup	Command: cyap_status	Command: disable_ipv6_support	Command: wireless_info
Scheduled Tasks			
Mount Points			
Backup / Flash Firmware	Run Download	Run Download	Run Download
Custom Commands			
License	ICCP Config	Modem Information	Modem Manager Debug
Reboot	Command: cfg_iccp	Command: modem info	Command: modemmanager debug
Ignition Timer	Arguments:		Arguments:
VPN	Argumenta.		Alguments.
Services	Run Download	Run Download	Run Download
Network			
Statistics	Modem Gateway	Modem Speedtest	Modem Factory Reset
	Command: modem_gateway	Command: modem_speedtest	Command: modem_factory_reset
Logout	Arguments:	Arguments:	Arguments:
	Run Download	Run Download	Run Download
	<pre># "disable_ipv6_support"</pre>		
	This script will remove IPv6 sup This script only needs to run or and 'dhcp'. Firewall rules with As finished the firewall IPv6 to This is the first call without a Command failed (Code: 256)	rce. New settings are saved to ' family=ipv6 are removed form co raffic counters should be zero.	network' nfiguration.

Disable network IPv6 support - first run

5.3 Example: Local Access Point

As a first step, a simple access point is configured. The wired Ethernet and the wireless radios form an isolated local domain where the CyBox AP 3 provides DHCP services. Finally the example in "LAN IP Address" shows how to set a new static IP address. In Network > Interfaces \rightarrow LAN \rightarrow Protocol you can configure the DHCP client setup to obtain an IP address from a DHCP server in your network. The access point and its clients become part of another local domain where DHCP, DNS, and a gateway are provided, connecting the CyBox AP 3 and its clients to higher-level networks.

5.3.1 System Settings

- Select $System \rightarrow System$ (yes, two System tabs nested).
- In box System Properties select tab General Settings: adjust the entries as needed; button Sync with browser is useful for cases where no NTP server is available. Tabs Logging and Language and Style may be ignored for now.
- In the tab Time Synchronization: adjust the entries if needed.
- Click button Save & Apply

5.3.2 Prepare WLAN Radio Interface

• Select Network → Wireless: this shows the wireless controllers *radio0* and *radio1* with some software buttons

ELTEC

systems

- Select tab radio0: Unknown "OpenWrt" or click the Edit button of radio0
- In box Device Configuration:
 - Select tab Advanced Settings
 - In drop-down menu Country Code, select the country of the current location
 - Select tab General Setup
 - In drop-down menu *Mode*, select a mode, usually *N* or *AC*
 - In drop-down menu *Channel*, select a channel (or *auto*)
 - If needed, select an appropriate value in drop-down menu Transmit Power
- In box Interface Configuration:
 - [Select tab General Setup]
 - Enter an arbitrary ESSID (will be quoted below as "WLssid")
 - [Mode: select Access Point]
 - [Field Network: activate checkbox lan]
 - [Field *Network*: clear checkbox *create*]
 - If needed, activate checkbox Hide ESSID
 - Select tab Wireless Security
 - In drop-down menu Encryption, select as needed
 - In drop-down menu Cipher, select auto unless a specific algorithm is required
 - Enter encryption Key at least 8 characters
- Click button *Save* & *Apply*
- Select Network → Wireless
 - For radio0, click button Enable

At this point, the radio interface should become visible to possible WLAN clients and vice versa. Probably clients need to be prompted to scan for available wireless networks. Then, those clients will become visible in tab *Network*, tab *WiFi*, box *Associated Stations*.

5.3.3 Connect radio0 to the Network

- Select tab Network tab Interfaces tab LAN
- In box Common Configuration
 - Select tab *Physical Settings*:
 - *Bridge interfaces*: activate checkbox
 - [Enable STP: clear checkbox Spanning Tree Protocol on this bridge]
 - [Interface : activate checkbox Ethernet Adapter: "eth0"]

- Interface : activate checkbox Wireless Network: Master "<SSID>"
- [Interface : clear checkbox Custom Interface]
- In box DHCP Server
 - Select tab General Setup
 - Clear checkbox Disable DHCP for this interface
 - If needed, modify more things in tab *General Setup* and tab *Advanced Settings*
- Click button Save & Apply

Now the CyBox AP 3 connects the Ethernet and all WLAN clients in the local domain 192.186.100.0 and provides a local DHCP service, but there is not yet an uplink to a gateway.

5.3.4 Connecting to WAN

As a goal, the CyBox AP 3 shall integrate its clients via Ethernet in a higher-level network. DHCP, DNS, and gateway services are supposed to be available in that net.

- Select tab Network tab Interfaces tab LAN
- In section Common Configuration:
 - In drop-down menu Protocol, select DHCP Client
 - Click button Switch Protocol
- Click button *Save* & *Apply*

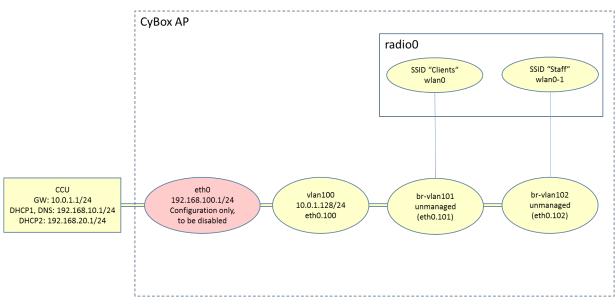
This terminates the local domain 192.186.100.0. Now connect the CyBox AP 3 via Ethernet to the gateway domain, restart the CyBox AP 3 (use hardware reset switch) and reconnect the WLAN clients.

5.4 Example: Connecting three VLANs to a server

In this use-case the access point provides 3 VLAN interfaces:

- one for management access via wired Ethernet, using a static IP address
- an unmanaged WLAN access for "clients", no encryption
- another unmanaged WLAN access for "staff" members, encrypted, optional hidden SSID

The access point is connected via Ethernet to a server (or a host computer, called CCU in the illustration below) providing DHCP, DNS, and gateway services. Starting from factory defaults, apply system settings as described in section 7.2.1 (if needed).



Network Topology with Three VLANs

5.4.1 Create the Management VLAN

Create a new Ethernet interface (eth0.100) and give it the name "vlan100". Make it a full-valued net host by assigning a static address and a gateway.

- Select tab Network tab Interfaces
- Click button Add new interface
- Enter Name of new interface: "vlan100"
- [Select Protocol of the new interface: Static address]
- [Clear checkbox "Create a bridge over multiple interfaces"]
- Enter name of Custom Interface: "eth0.100"
- Click button Submit
- [page VLAN100 opens]
- [Tab Network tab Interfaces tab VLAN100 tab General Setup]
 - Enter IPv4 address "10.0.1.128"
 - Select IPv4 netmask 255.255.255.0
 - Enter IPv4 gateway "10.0.1.1"
- Click button Save & Apply

5.4.2 Add two unmanaged VLANs

We create 2 more Ethernet interfaces eth0.101 and eth0.102 with names vlan101 and vlan102, resp.

- Network Interfaces: Add new interface → Name of new interface: "vlan101"
- Protocol of new interface: Unmanaged
- [Clear Create a bridge over multiple interfaces]
- Custom Interface: "eth0.101 "

- Submit
- [page VLAN101 opens]
- Click button Save & Apply

Do the same for "vlan102" and "eth0.102".

5.4.3 Configure and Enable the radio(s)

You are free which interface to assign to which radio. If both radios are to be used then this section (7.3.3) must be done for *radio1* as well.

- Select tab Network -> tab WiFi -> tab radio0 (or click button Edit for radio0)
- In box Device Configuration:
 - Select tab Advanced Settings
 - Select Country Code
 - Select Mode

The following 3 lines fix a problem with this LuCI page (The drop-down menu for the country code is not updated correctly)

- Click button Save & Apply
- Logout / Login
- Select tab Network -> tab WiFi -> tab radio0 (or click button Edit for radio0)

Now we can complete the configuration for *radio0*:

- In box Device Configuration:
 - Select tab Advanced Settings
 - Select HT mode
 - Select Channel
 - Select Transmit Power
- Click button *Save & Apply*
- Select tab Network -> tab WiFi
- Click button Enable for radio0

5.4.4 Attach the "Clients" VLAN to radio0

- Select tab *Network* -> tab *WiFi* -> tab *radio0* (or click button *Edit* for *radio0*)
- In box Interface Configuration:
 - [Select tab General Setup]
 - Enter ESSID "Clients"
 - Clear checkbox lan
 - Activate checkbox *vlan101*

Click button Save & Apply

5.4.5 Attach the "Staff" VLAN to radio0

- Select tab Network tab WiFi
- Click button Add for radio0 (if both VLANs shall run on the same radio).

Alternatively, if the "Staff" shall use the other radio and that radio has been configured and enabled (see 7.3.3), then (instead of *Add*) select tab *Network* tab *WiFi* tab *radio1* (or click button *Edit* for *radio1*)

- In box Interface Configuration:
 - [Select tab General Setup]
 - Enter ESSID "Staff"
 - [Clear checkbox lan]
 - Activate checkbox vlan102
 - If needed, set checkbox Hide ESSID
 - Select tab Wireless Security
 - Select Encryption (e.g. WPA2-PSK)
 - Enter Key (at least 8 characters)
- Click button Save & Apply

5.4.6 Check Configuration

As a check, you may login to the CyBox AP 3 through SSH and issue the ifconfig command. The following interfaces should be shown:

```
br-vlan101 Link encap:Ethernet ...
br-vlan102 Link encap:Ethernet ...
eth0 Link encap:Ethernet
inet addr:192.168.100.1 Bcast:192.168.100.255 Mask:255.255.255.0
...
eth0.100 Link encap:Ethernet
inet addr:10.0.1.128 Bcast:10.0.1.255 Mask:255.255.255.0
...
eth0.101 Link encap:Ethernet ...
eth0.102 Link encap:Ethernet ...
lo Link encap:Local Loopback ...
wlan0 Link encap:Ethernet ...
wlan0-1 Link encap:Ethernet ...
```

Oder alternativ (anstelle von wlan0-1), wenn beide Funkmodule verwendet werden:

wlan1 Link encap:Ethernet ...

5.4.7 Disable Unneeded Default Address

After successfully testing the VLAN-based management access (vlan100), the default address 192.168.100.1 may be disabled. This is easily achieved by deleting the *LAN* interface:

- Select tab Network tab Interface
- Click button Delete for the LAN interface (usually the lowermost)
- Select tab Network tab Interfaces tab LAN

Alternatively, you may change the protocol of the LAN interface to Unmanaged:

- Select tab Network tab Interface tab LAN
- In box Common Configuration:

• In drop-down menu Protocol select Unmanaged

Click button Save & Apply

5.5 Example: Client Isolation within the Access Point

By default, all clients of an access point can directly communicate with each other. Depending on the use case, this might be undesirable.

5.5.1 Isolate the Radio Clients

- Select tab Network -> tab WiFi -> tab radio0 (or click button Edit for radio0)
- In box Interface configuration
 - Select tab Advanced settings
 - Activate checkbox Separate clients
- Click button Save & Apply
- Do the same for the other radio

5.5.2 Restrict Access to Local Ports to Specified Interfaces

- Select tab System tab Administration
- In box Dropbear Instance
 - Click radio button lan
 - [unselect radio button unspecified]
- Click button *Save* & *Apply*

This affects the mentioned port only. To protect more ports against WLAN access, use button Add.

Note that all interfaces listed in the *lan* field are allowed to access the respective socket.

6 THE WEB INTERFACE

Most pages of the web interface are concerned with the configuration of the CyBox AP 3. Many of these pages show some of the following buttons:

- Reset: clicking on this button reverts the unsaved input fields of the current page to the values as they were before you modified them.
- Save: This button copies the modified input fields of the current page to an intermediate memory. It collects changes without applying them to the CyBox AP 3. This is important because some changes if applied stand-alone could break the IP connection between host and the CyBox AP 3.

When clicking this button, a change count notification appears at the upper left, indicating the number of to-be-changed lines in the configuration data (The actual text in that message is kind of misleading: it claims to state the number of "unsaved changes" but actually means the number of saved but not yet applied new configuration lines.)

It should be noted, that saved data are not longer subject to the *Reset* button. Rather, saved changes - if not applied - are kept until you click the Save & Apply button, or the Revert button (see below), or CyBox AP 3 reboots. The configuration is not yet complete as long as the change count is non-zero.

- Revert: Clicking on the change count message pops up an extra window showing the data exactly as they would be entered into the related configuration files. This window provides a button named Revert. Clicking it invalidates the saved changes and clears the change count to zero.
- Save & Apply: this button performs the *Save* operation (see above), modifies the configuration data according to the saved changes, and clears the change count. Please note that **Revert** and **Reset** cannot undo those changes after a *Save* & *Apply* operation! Also, depending on the specific parameters changed, networking interfaces are re-initialized with the new data. In consequence, the host-side browser might require to connect a new IP address to access the CyBox AP 3.
- Submit: Some pages provide a single Submit button instead of the above. Essentially, Submit performs an immediate Save operation. Thus, the change count in the upper left corner of the screen will increment. The Save operation also takes place when clicking special buttons like Add new interface or Setup DHCP Server. Again, the change count will change. In these cases, Save & Apply is needed to complete the operation.
- Buttons named Enable or Disable cause immediate execution.

6.1 Network

6.1.1 Interfaces

6.1.1.1 DHCP Server per Interface

A DHCP server can run on the device to assign IPv4 addresses to WLAN clients. It is enabled by unchecking *Disable DHCP for this interface*. However, DHCP often is managed by a dedicated DHCP server on the backbone and not directly on the access point. In that case, the DHCP server on the access point must be disabled.

6.1.1.2 Bridges

Physical network interfaces may be bridged to form a "software Ethernet switch". For example, by bridging the LAN 1 interface with a wireless interface, WLAN clients can communicate with LAN clients like they were connected by a switch.

To set up a bridge, use the tab Network \rightarrow Interfaces \rightarrow LAN \rightarrow section Common Configuration \rightarrow Physical Settings. Check Bridge interfaces and include all *Interfaces* that should belong to the new bridge interface.

The example Bridge Interface Setup shows a bridge containing "Ethernet Adapter: eth0" and "wlan0" (Wireless Network: Master "System-radio0").

systems

Interfaces » LAN				
General Settings Advanced Settings	Physical Settings	Firewall Settings	DHCP Server	_
Bridge interfaces				
	Creates a bridge	over specified interfa	ice(s)	tart
Enable STP				
	Enables the Spar	nning Tree Protocol (on this bridge	
Enable IGMP snooping				art
	Enables IGMP sr	nooping on this bridg	e	
Interface	🛃 eth0 🖉	🧶 wlan0	•	
	🗍 🧾 Ethernet Adap	oter: "bond0"		
1	Ethernet Adag	oter: "bonding_maste	ers"	
2 Pkts.)	Ethernet Adap	oter: "dummy0"		
29/24	Ethernet Adap	oter: "erspan0"		
iddress 13s	🛛 🚂 Ethernet Adap	oter: "eth0" (lan, lan_	alias, lan_dhcp, la	n_mac)
4:AE:4D -2 Pkts.)	Ethernet Adap	oter: "eth1" (wan, wa	n6)	
2 Pkts.)	Service Wireless Network	vork: Master "Systen	n-radio0" (lan)	
/8	C Wireless Netw	vork: Master "System	n-radio1" (lan)	
client 4:AE:4E	custom			

Bridge Interface Setup

Note: Physical interfaces, as eth0 or wlan0, belonging to a network interface, such as LAN, cannot be in any other network interface.

6.1.1.3 VLAN

To enable VLAN (virtual LAN, mostly used for logical subnets built on real LANs) tagging, a new custom interface must be set up for the *LAN*. The VLAN interfaces are named e.g. "eth0.12". In this example "12" is the VLAN tag to be used.

Name	vlan12
Protocol	Static address
Bridge interfaces	creates a bridge over specified interface(s)
Interface	🗾 @lan 🔻
	unspecified
	Ethernet Adapter: "bond0"
ent	Ethernet Adapter: "bonding_masters"
	Ethernet Adapter: "dummy0"
E:4D Pkts.)	Ethernet Adapter: "erspan0"
Pkts.)	🤰 Ethernet Adapter: "eth0" (lan, lan_alias, lan_dhcp, lan_ma
/24 ress	Ethernet Adapter: "eth1" (wan, wan6)
less	👷 Wireless Network: Master "System-radio0" (lan)
E:4D Pkts.)	👷 Wireless Network: Master "System-radio1" (lan)
Pkts.)	😥 Alias Interface: "@lan"
	🔊 Alias Interface: "@lan_alias"
ent E:4E	Alias Interface: "@lan_dhcp"
L.7L	Alias Interface: "@lan_mac"
	Alias Interface: "@wan"
dient E:4E	Alias Interface: "@wan6"

VLAN interface setup

Use *eth0.X* as custom interface and disable *eth0* as shown in the dialog above.

WARNING: After saving and applying the changes, the network output on *eth0* is tagged with your VLAN tag and the AP will not be accessible through normal network anymore. You need to enable VLAN tagging on the host interface, or connect to a switch that is able to handle this VLAN tag to be able to access the AP.

6.1.2 WLAN

Wireless radios are disabled by default to avoid erroneous WLAN operation. Use $Network \rightarrow Wireless \rightarrow Edit$ to enter the configuration menu. Details about WLAN configuration can be found in the next section. After configuration, enable the interfaces with Enable.

Status	Wireless Overview	N					
System							
VPN	👳 radio0	Qualcomm Atheros Channel: 36 (5.180 GHz		J2.11bgnac	Restart	Scan	Add
Services	/-99 dBm	SSID: System-radio0 M BSSID: 04:F0:21:2E:49:			Disable	Edit	Remove
Network	👳 radio1	Qualcomm Atheros Channel: 36 (5.180 GHz		02.11bgnac	Restart	Scan	Add
Interfaces		SSID: System-radio1 M					
Wireless	/-102 dBm	BSSID: 04:F0:21:2E:49:		•	Disable	Edit	Remove
DHCP and DNS	Associated Station	ns					
Hostnames	Network	MAC-Address	Host	Signal / Noise	RX Rate / TX Rate	e	
Static Routes							
Firewall			No ii	nformation available			
Diagnostics					Save &	Appi 🔽 😫	Save Reset
Configure Diagnostics							
Load Balancing							
Connection Check							
Client Isolation							
QoS							
Statistics							
Logout							

Wireless Device Overview

The example shows a CyBox AP 3 with two radios installed. Depending on the hardware, other configurations may be shown.

After enabling the radio, you can configure physical settings. Clicking $Network \rightarrow Wireless \rightarrow Edit$ redirects you to the 'Device Configuration' menu.

6.1.2.1 Channel, Wireless mode, HT mode, Power settings

Advanced Settings allows to select the appropriate country in the pull-down menu. After a country change, press the *Save & Apply* button, refresh the browser page, and reboot.

Disclaimer: The wireless configuration must observe the local regulation. The upper limit of the transmission power has to be set correctly ("Transmit power"). This does not account for an antenna gain. If, for example, the regulation imposes a maximal power of 15 dBm and the gain of the antenna is 5 dBm, you must set the transmit power to a value at or below 10 dBm.

In *General Setup* you can configure wireless mode, HT mode and channel. Wireless mode can be forced to any 802.11 standard supported by the radio. The channel selection is adapted to the wireless mode chosen. The channel configuration can be set to auto but this slows down WLAN activation and requires a reboot to work properly. Therefore, it is recommended to select a defined channel.

General Setup	Advanced Settings	5
Status		Mode: Master SSID: System-radio0 BSSID: 04:F0:21:2E:49:B5 Encryption: None /-94 dBm [*] Tx-Power: 23 dBm Signal: 0 dBm Noise: -94 dBm Bitrate: 0.0 Mbit/s Country: DE
Wireless networ	k is enabled	Disable
Operating frequ	ency	Mode Channel Width AC • 36 (5180 Mhz) • 80 MHz •
nterface Con	figuration	Specifies the maximum transmit power the wireless radio may use. Depending on regulato requirements and wireless usage, the actual transmit power may be reduced by the driver.
nterface Con General Setup	figuration	wireless radio may use. Depending on regulato requirements and wireless usage, the actual
		wireless radio may use. Depending on regulato requirements and wireless usage, the actual transmit power may be reduced by the driver.
General Setup		wireless radio may use. Depending on regulato requirements and wireless usage, the actual transmit power may be reduced by the driver.
General Setup Mode		wireless radio may use. Depending on regulato requirements and wireless usage, the actual transmit power may be reduced by the driver.
General Setup Mode ESSID		wireless radio may use. Depending on regulato requirements and wireless usage, the actual transmit power may be reduced by the driver.

Wireless Device Configuration

After the device has been enabled, the radio status should be checked if the selected channel / mode combination is working.

6.1.2.2 Radio Band Configuration for Models with Antenna Combiner

If the system is equipped with an antenna combiner, (e.g. having two radio modules (WLE-900) but only three antennas) the frequency bands 2.4 GHz and 5 GHz cannot be freely configured for each wireless module. The first radio module radio0 must use band 2.4 GHz and the second radio radio1 the 5 GHz band. An incorrect wireless band configuration in the software is possible. However, this means that no output power arrives at the antenna ports.

6.1.2.3 JJPlus Radio Card Band Configuration

If system is equipped with a **JJPlus Wave-2** radio module, the frequency band 2.4 GHz and 5 Ghz cannot be switched on the fly (runtime) in the wireless configuration menu. After a *Factory Reset* the radio modules are configured for 5 GHz as default band. To switch to the 2.4 GHz band a **Custom Command=>Switch RadioX Band** must be executed and after that a system reboot must be triggered. The 2.4 GHz mode then, will be permanently stored in the configuration backup archive. Executing the custom command button again will toggle from 2.4 GHz to 5 GHz and vice versa. The selected mode is always stored in the configuration backup archive. Note that a band toggle will always *disable* the selected radioX. After reboot the selected radioX must be activated again and the channel/bandwidth must be configured.

Status	Dashboard Configure		
System	Custom Commands		
System			
Administration	System Information	System IPv6 Disable	Wireless Info
Startup	Command: cyap_status	Command:disable_ipv6_support	Command:wireless_info
Scheduled Tasks Mount Points			
LED Configuration			
Backup / Flash Firmware	Run Download	Run Download	Run Download
Custom Commands			
Reboot	ICCP Config	Switch Radio0 Band	Switch Radio1 Band
VPN	Command: cfg_iccp	Command:jjplus_switch_band 0	Command:jjplus_switch_band 1
Services	Arguments:		
Network	Run Download	Run Download	Run Download
Statistics			
	Select Routing App (!RESET ALL	Get Active Routing App	
Logout	• • • •		-
	CONFIGURATIONS!)	Command: routing_get	
	Command: routing_set		
	Run Download	Run Download	

JJPlus Wave-2 Frequency Band Toggle

6.1.2.4 ESSID, WDS Mode, Client separation

The ESSID is used for WLAN clients to select the wireless LAN by name. Set up a ESSID name for the wireless network in the *General Setup* of the *Interface configuration* and use mode *Access Point*.

A Wireless Distribution System (WDS) can be set up by using two access points with the same ESSID, one in "Access Point (WDS)" mode and the other in "Client (WDS)" mode. This mode is required for the Inter Carriage Connection Protocol (ICCP).

In public access point environments the client-to-client communication should be prevented by activating the Interface Configuration \Rightarrow Advanced Settings \Rightarrow Isolate Clients checkbox. Note that this configuration only prevents the communication between clients connected to the same access point. In a backbone with many access points having the same SSID, an additional "Client isolation" function between APs is needed (see 6.1.2.8 Multi-AP Client Isolation).

6.1.2.5 Encryption

On the tab Wireless Security you can choose a security mode. The following modes are supported:

- WPA3 (strong security)
 - WPA3-SAE: "personal mode", using a key (password) for access.
 - WPA3-EAP: "enterprise mode", using a RADIUS server for client authentication.
- WPA2 (strong security)
 - WPA2-PSK: "personal mode", using a password for access. Note that the cipher "TKIP" is considered insecure, and CCMP should be used instead.
 - WPA2-EAP: "enterprise mode", using a RADIUS server for client authentication.
- WPA (medium security)
 - WPA-PSK: WPA in "personal mode", using a password for access. Note that the cipher "TKIP" is considered insecure, and CCMP should be used instead.
 - WPA-EAP: "enterprise mode", using a RADIUS server for client authentication.
- WEP (weak security)

- WEP Shared Key
- WEP-EAP Open System
- OWE (open, encrypted)
 - OWE: The "Opportunistic Wireless Encryption" mode requires no password, yet the WLAN traffic is encrypted. This mode is intended for public access points.
- No Encryption (open):
 - The WLAN traffic is not secured at all.

In addition, some of these modes can be combined ("mixed mode"). For an access point, this allows to support multiple modes, supporting newer encryption standards while still supported older clients. When configuring the CyBox AP 3 as client with a "mixed mode", it will try both modes when connecting to an access point (normally, only the configured mode is used). The following modes can be combined:

- WPA3 and WPA2 in enterprise mode (EAP)
- WPA3 and WPA2 in personal mode (PSK respective SAE)
- WPA2 and WPA in personal mode (PSK)

evice Configuration	
General Setup Advanced Settings	
Status	Mode: Master SSID: System-radio0 BSSID: 04:F0:21:2E:49:B5 Encryption: None Channel: 36 (5.180 GHz) /-94 dBm Tx-Power: 23 dBm Signal: 0 dBm Noise: -94 dBm
	WPA2-PSK (strong security)
Wireless network is enabled	WPA2-EAP (strong security)
	WPA3-EAP (strong security)
	WPA2-EAP/WPA3-EAP Mixed Mode (strong security)
Operating frequency	WPA3-SAE (strong security)
Maximum transmit power	WPA2-PSK/WPA3-SAE Mixed Mode (strong security)
	WPA-PSK/WPA2-PSK Mixed Mode (medium security)
	WPA-PSK (medium security)
	WPA-EAP (medium security)
	WEP Open System (weak security)
nterface Configuration	WEP Shared Key (weak security)
	OWE (open network)
General Setup Wireless Security	No Encryption (open network)
Encryption	No Encryption (open network)

Wireless Device Configuration – Encryption Settings

6.1.2.6 Hotspot 2.0

The CyBox AP 3 supports Hotspot 2.0 (Release 1), which is configured on the tab Hotspot 2.0.

Note
The Hotspot 2.0 tab is only present if
• The WLAN is configured as AP
• The encryption mode uses RADIUS (i.e. EAP)
SP/HO

Hotspot 2.0 separates the hotspot operator from the service providers. The hotspot operator maintains the access point offering Hotspot 2.0 services while the service providers are responsible for authentication and authorization of WLAN clients. It is possible to configure multiple service providers on a single access point.

Each hotspot operator has one or more domain names, which can be configured in the Domain Names setting.

Service providers are identified by one of the following:

- Consortium IDs: Numeric values assigned by the IEEE. Each ID names a consortium of multiple service providers.
- NAI Realms: The domain names of the service providers. Optionally, the authentication scheme can be appended to each name. The WLAN clients can fetch this information prior before they connect.
- 3GPP Cell Identifiers: Each cell ID consists of the MCC and MNC of a service provider. A mobile device can seamlessly roam between mobile networks and WLAN by identifying its mobile network provider on a Hotspot 2.0 access point.

At least one of these three parameters must be configured.

The Operator Friendly Name is the access point operators name. It is intended to be presented to human users of WLAN clients. Multiple entries can be configured to present the name in different languages.

The Venue Group and Venue Type settings classify the type of the venue in which the access point is installed. This might be a coffee shop, for example. The possible values are defined in IEEE Std 802.11u-2011.

The Venue Name might be presented to human users. It can be configured for multiple languages.

The Network Access Type describe the type of the offered network access. The Internet is available indicates whether internet access is available from this access point. Both are presented to WLAN clients before they connect.

The ANQP Domain ID can be used to group multiple access points which reside in the same ESS (Extended Service Set).

The Additional ANQP Elements setting allows to add elements.

6.1.2.7 WLAN Clients test

After setup is completed, the access point is ready to associate WLAN clients to the local network.

6.1.2.8 Multi-AP Client Isolation

Client separation inhibits direct communication between clients of the same WLAN radio. However, if more than one Access Point is attached to the same cable backbone, and the wifi clients use the same subnet, client isolation must also be enabled between APs. This is also true if the CyBox AP 3 operates multiple APs on different WLAN modules which are connected (e.g. by using a bridge). Isolation is also done for clients on different radios within the same Access Points.

In order to use Multi-AP client isolation, all APs must use the same Server and use the same interface name. (Network traffic can be restricted with a configuration for 'ebtables' on FORWARD rules, managed by the 'client isolation' functionality).

For Client isolation over APs, check Network \rightarrow Client Isolation \rightarrow Enable, then enter parameters for your configuration.

The screenshot below shows a configuration where the server address is set in the parameters of the LAN interface (under '*Network*' \rightarrow '*Interfaces*'). When the interface is set up as a bridge, the corresponding Bridge name is always 'br-<original_interface_name>'

Status	Client Isolation		
System	Network Isolation for WiFi clients on different APs connected to same backbone. Isolation is also done for clients on different radios within the same AP.		
VPN Services	Network Isolation Settings		
Network	Enable		
Interfaces		Enable client isolation service	
Wireless	Server address list	192.168.100.100 172.16.0.100	
DHCP and DNS		O Specifies the server or server list for MAC address requests	
Hostnames Static Routes	Device	br-lan	
Diagnostics Firewall		Specifies the physical device for arping test requests	
Client Isolation	SSID list to isolate	Please choose CyBoxAP-2-radio0	
Connection Check QoS		CyBoxAP-2-radio1	
Configure Diagnostics		Select one or more SSIDs for isolation rules	
Statistics	Allowed MAC address list		
Logout		Specifies a comma separated list of allowed MAC addresses	
	Timeout	20	
		Maximum time in seconds to wait for server reaction	
	Wait time	120	
		Ime in seconds to wait before a new server list scan starts	
		Save & Apply Save Reset	

Client isolation across access points

6.1.2.9 Connection Check

The connection check service allows to disable WLANs while no internet connectivity is possible. This can improve the user experience by avoiding being connected to a WLAN which delivers no internet connectivity.

The connection check works by issuing an *arping* to the server. When the server cannot be reached, the WLAN gets deactivated. Otherwise, the WLAN gets activated. The service can be configured on the page $Network \rightarrow Connection$ Check (see figure "Deactivate SSIDs when the server is not reachable" below). The checkbox Enable enables or disables it.

The parameter Server address determines which address is arpinged to determine whether the connection is healthy. The parameter Interface name dictates which interface to use for the arping. Note that this is a physical interface, such as br-lan or eth0.

In the SSID list, the controlled SSIDs can be chosen. The selected SSIDs are activated or deactivated by the service, while the others remain unaffected.

The connection is checked every Check time interval seconds. The selected SSIDs are disabled when the connection was down for at least Shutdown time seconds, and they are enabled again when the connection was healthy for at least Activate time seconds. Note that the latter two work at the granularity of Check time interval \Rightarrow 15s and Activate time \Rightarrow 20s, the WLANs will be activated after the 2nd successful check, i.e. after 30s.

Status	Connection Check		
System	Connection Check allows to enable/disable wifi SSIDs depending on server accessibility		
VPN	Connection Check Settings		
Services			
Network	Enable		
Interfaces		Provide the second s	
Wireless	Server address	192.168.100.100	
DHCP and DNS Hostnames		Specifies the server for MAC address requests	
Static Routes	Interface name	br-lan	
Diagnostics Firewall		Specifies the interface for arping test requests	
Client Isolation	SSID list	Please choose	
Connection Check		CyBoxAP-2-radio0 CyBoxAP-2-radio1	
QoS			
Configure Diagnostics			
Load Balancing		Ø Select one or more SSIDs for connection check	
Statistics	Check time interval	20	
Logout		Wait time (seconds) between two connection checks	
	Activate time	60	
		Wait time (seconds) before wifi is activated after connection valid	
	Shutdown time	60	
		Wait time (seconds) before wifi shutdown after connection invalid	
		Save & Apply Save Reset	

Deactivate SSIDs when the server is not reachable

6.1.2.10 Access Point Scanning Service (Wireless Monitoring)

Reporting nearby APs to interested parties

Important

A **must** precondition to use this service is to have at least one available radio device running AP (AccessPoint) mode. Please make sure, such configuration is done and running **before** activating this service. Otherwise no scanning results can be obtained.

Since service is activated (enabled), scanning is done continiously in the background. All channels of selected radio device(s) are scanned one after another. Scan results are stored to a temporarily FIFO queue and can be obtained anytime.

The scanning service is configurable over UCI resp. LUCI. A separate page (Services -> AP Scanner) can be used to configure radio devices which are used for scanning. Also the interval between scanning cycles and the maximum queue length can be configured.

Important

System load and network traffic caused by SNMP calls can be minimized by using of SSID filter parameters. As long SSID filter is enabled, only entries matching the predefined filter will be stored to a result queue.

Status	Wireless Monitoring			
System				
VPN	Settings			
Services	Enable			
Customize	Radio interface list (Access Point)	Please choose		
SNMPD		radio0		
SNMPD Edit				
SNMP-Trap		Select one or more radios for scanning		
GPS Info	Activate SSID Filter			
GPSD		disable		
Shadowsocks-libev	Interval between scanning cycles (seconds)	5		
SMS Command	Data Queue length	1000		
ICCP		1000		
AP Scanner		Save & Apply Save Reset		

Scanning results can be obtained by a SNMP request. Request configuration can also be done by using of UI page (Services->SNMPD Edit).

Status	SNMPD Edit
System	This is the content of /etc/config/snmpd. Modify or remove sections for security reasons.
VPN	
Services	option name 'gps_modem_raw'
Customize	option args '/var/run/gps/modem_gps.raw' option miboid '1.3.6.1.4.1.2021.8.1.2.158'
SNMPD	
SNMPD Edit	option name 'apscan data'
SNMP-Trap	option prog '/usr/sbin/get_queue_entry' option args 'apscan'
GPS Info	option miboid '1.3.6.1.4.1.2021.8.1.2.159'

Getting queue entry from remote host

In case of empty queue respone will be a "nil" value.

```
~# snmpget -c public -v 2c <device_ip> 1.3.6.1.4.1.2021.8.1.2.159.101.1; iso.3.6.1.4.1.2021.8.1.2.159.101.1 = STRING: "nil"
```

Important

As soon queue has reached the configured maximum length, every time there is a new entry added to queue the "oldest" one will be dropped!

How to avoid data lost?

- 1. increase maximum queue length
- 2. collect sampled data more often e.g. once a second (snmp request)

Scanning results are stored in CSV format:

- S_BSSID (MAC of scanner radio)
- SSID (the name)
- BSSID (the MAC)
- channel
- signal level
- "last seen" timestamp

Current queue status (entries) can be also discovered on the UI page (Status->AP Scanner).

Status	Scanner Results
Overview	00.13.01.20.NC.00.00011.00.1.00.00.00.00.00.00.00.00.0
Advanced	"00:15:61:20:AC:8A;DIRECT-29-HP OfficeJet 6950;C8:D9:D2:C7:DB:2A;6;-86;2021-01-11 11:36:28", "00:15:61:20:AC:8A:HR:90:72:40:22:23:48:6:-76:2021-01-11 11:36:28",
Firewall	"00:15:61:20:AC:8A;devolo-0b2;30:D3:2D:B7:D0:B2;8;-84;2021-01-11 11:36:29",
Routes	"00:15:61:20:AC:8A;Telekom_FON;4C:1B:86:A3:12:46;11;-91;2021-01-11 11:36:29", "00:15:61:20:AC:8A;FRITZ!Box Gastzugang;0A:96:D7:2A:B7:91;11;-90;2021-01-11 11:36:29",
System Log	"00:15:61:20:AC:8A;Westerwald;08:96:D7:2A:B7:91;11;-90;2021-01-11 11:36:29", "00:15:61:20:AC:8A;WLAN-344368;D4:21:22:9F:86:F3:1:-85:2021-01-11 11:36:35",
Kernel Log	"00:15:61:20:AC:6A;WLAN-344368;D4:21:22:97:80:F5;1;-65;2021-01-11 11:30:35 , "00:15:61:20:AC:8A;vmn;3C:A6:2F:26:9D:5D;1;-53;2021-01-11 11:36:35",
5	"00:15:61:20:AC:8A;vmn;3C:A6:2F:B9:F8:2C;1;-72;2021-01-11 11:36:35", "00:15:61:20:AC:8A;vmn;24:65:11:3D:9E:CE;1:-85:2021-01-11 11:36:35",
Processes	"00:15:61:20:AC:6A;VWLAN-344368;F0:B0:14:F3:C3:09;1;-89;2021-01-11 11:36:35",
Realtime Graphs	"00:15:61:20:AC:8A;Zorni;E0:28:6D:BA:67:D9;1;-89;2021-01-11 11:36:35",
AP Scanner	"00:15:61:20:AC:8A;PowerFernseher;24:65:11:CF:A9:5C;1;-87;2021-01-11 11:36:35", "00:15:61:20:AC:8A;Telekom FON;9C:C1:72:D5:17:01;1;-90;2021-01-11 11:36:35",
Rogue AP	"00:15:61:20:AC:8A;SHFUNK;9C:C1:72:D5:17:00;1;-90;2021-01-11 11:36:35", "00:15:61:20:AC:8A:HR:D0:03:4B:65:D8:DA;1:-91:2021-01-11 11:36:35",
System	"00:15:61:20:AC:8A;HR;D0:03:4B:05:D0:DA;1;-91;201-01-11 11:30:35 ; "00:15:61:20:AC:8A;Ulli;7C:FF:4D:E4:5E:8A;1;-88;2021-01-11 11:36:35",
, ,	"00:15:61:20:AC:8A;DIRECT-29-HP OfficeJet 6950;C8:D9:D2:C7:DB:2A;6;-87;2021-01-11 11:36:36", "00:15:61:20:AC:8A:HR:90:72:40:22:23:48:6:-75:2021-01-11 11:36:36",
VPN	"00:15:61:20:AC:8A;Advolo-0b2;30:D3:2D:B7:D0:B2;8;-84;2021-01-11 11:36:37",
Services	"00:15:61:20:AC:8A;Telekom_FON;4C:1B:86:A3:12:46;11;-90;2021-01-11 11:36:38", "00:15:61:20:AC:8A;FRITZ!Box Gastzugang;0A:96:D7:2A:B7:91;11;-91;2021-01-11 11:36:38",
Network	"00:15:61:20:AC:8A;HAT2:Box Gast2dgang;GA:90:D7:2A:87:91;11; 91;2021-01-11 11:36:38", "00:15:61:20:AC:8A;Westerwald;08:96:D7:2A:B7:91;11; -90;2021-01-11 11:36:38",
Statistics	"00:15:61:20:AC:8A;BVB09;4C:1B:86:A3:12:44;11;-90;2021-01-11 11:36:38",
Statistics	7

6.1.2.11 Client Counting Service

Reporting nearby Clients to interested parties

Important

A **must** precondition to use this service is to have at least one available radio device running AP (AccessPoint) mode. Please make sure, such configuration is done and running **before** activating this service. Otherwise no sniffed results can be obtained.

Since the service is activated (enabled), sniffing is done continiously in the background. A special monitor device is created for selected radio interface(s). Data received by radio interface (AP) also goes throw the monitor device. Probe Requests sent by clients around the monitor device are used for definitely client identification. Sniffed personal data (MAC and SSID) have to be protected according to the requirements of personal data protection regulations (DSGVO). Encryption algorith uses additional String (Pepper), configured by user, to achieve better anonymization results. Also there is a mechanism to encrypt personal data up to multiple times (hash_count). Results are stored to a temporarily FIFO queue and can be obtained anytime.

The sniffing service is configurable over UCI resp. LUCI. A separate page (Services -> WLAN Sniffer) can be used to configure radio devices which are used for sniffing. Also the maximum queue length, additional string and hash cycle count values can be configured.

Status	WLAN Client Counting			
System	Sattings			
VPN	Settings			
Services	Enable			
Customize	Radio interface list (Access Point)	Please choose radio0		
SNMPD		radio1		
SNMPD Edit		radio2		
SNMP-Trap		Select one or more radios for sniffing		
GPS Info	Data Queue length	1000		
GPSD		1000		
Rouge AP	Hash String (Pepper)	cYb0X_pePPer_KEy		
ICCP	Hash cycle count	5		
Wlan Sniffer				
Softflowd		Save & Apply Save Reset		

Results can be obtained by a SNMP request. Request configuration can also be done by using of UI page (Services->SNMPD Edit).

Status	SNMPD Edit
System	This is the content of /etc/config/snmpd. Modify or remove sections for security reasons.
VPN	This is the content of retocoming simple, would of remove sections for security reasons.
Services	option miboid '1.3.6.1.4.1.2021.8.1.2.159'
Customize	config exec
SNMPD	option name 'sniff_data' option prog '/usr/sbin/get queue entry'
SNMPD Edit	option args 'sniff' option miboid '1.3.6.1.4.1.2021.8.1.2.160'
SNMP-Trap	
GPS Info	##### assoclist0 Table0 objects #####

Getting queue entry from remote host.

In case of empty queue respone will be a "nil" value.

```
~# snmpget -c public -v 2c <device_ip> 1.3.6.1.4.1.2021.8.1.2.160.101.1; iso.3.6.1.4.1.2021.8.1.2.160.101.1 = STRING: "nil"
```

Important

As soon queue has reached the configured maximum length, every time there is a new entry added to queue the "oldest" one will be dropped!

How to avoid data lost?

- 1. increase maximum queue length
- 2. collect sampled data more often e.g. once a second (snmp request)

Sniffed results are stored in CSV format:

- radio device (which is used for sniffing e.g. radio0)
- MAC
- SSID (n/a for empty SSID)
- RSSI (signal level in dBm)
- "last seen" timestamp

Current queue status (entries) can be also discovered on the UI page (Status -> WLAN Sniffer).

Status	Sniffer Results
Overview	
Advanced	"radio1;c78236b5fb56b9023249e23e94dae7092aaa16f792aa168b21c064713b9883fe;n/a;-28dBm;2020-05-07 09:29:20", "radio1;f90a65957f2614491cc72284db4689020b2dbca102a237d0e94c10b7445cb4a4;n/a;-17dBm;2020-05-07 09:29:36",
Firewall	"radio1;c78236b5fb56b9023249e23e94dae7092aaa16f792aa168b21c064713b9883fe;n/a;-30dBm;2020-05-07 09:29:53", "radio1;c78236b5fb56b9023249e23e94dae7092aaa16f792aa168b21c064713b9883fe;n/a;-30dBm;2020-05-07 09:29:54",
Routes	"radio1;f90a65957f2614491cc72284db4689020b2dbca102a237d0e94c10b7445cb4a4;n/a;-16dBm;2020-05-07 09:30:10",
System Log	"radio1;c78236b5fb56b9023249e23e94dae7092aaa16f792aa168b21c064713b9883fe;n/a;-29dBm;2020-05-07 09:30:28", "radio1;c78236b5fb56b9023249e23e94dae7092aaa16f792aa168b21c064713b9883fe;n/a;-30dBm;2020-05-07 09:30:29",
Kernel Log	"radio1;f90a65957f2614491cc72284db4689020b2dbca102a237d0e94c10b7445cb4a4;n/a;-17dBm;2020-05-07 09:30:44", "radio1;c78236b5fb56b9023249e23e94dae7092aaa16f792aa168b21c064713b9883fe;n/a;-28dBm;2020-05-07 09:31:02",
Processes	"radio1;c78236b5fb56b9023249e23e94dae7092aaa16f792aa168b21c064713b9883fe;n/a;-28dBm;2020-05-07 09:31:03",
Realtime Graphs	"radio1;f90a65957f2614491cc72284db4689020b2dbca102a237d0e94c10b7445cb4a4;n/a;-16dBm;2020-05-07 09:31:18", "radio1;c78236b5fb56b9023249e23e94dae7092aaa16f792aa168b21c064713b9883fe;n/a;-29dBm;2020-05-07 09:31:36",
Rouge AP	"radio1;c78236b5fb56b9023249e23e94dae7092aaa16f792aa168b21c064713b9883fe;n/a;-29dBm;2020-05-07 09:31:37", "radio1:f90a65957f2614491cc72284db4689020b2dbca102a237d0e94c10b7445cb4a4:n/a:-18dBm:2020-05-07 09:31:53".
Wlan Sniffer	"radiol;c78236b5fb56b9023249e23e94dae7092aaa16f792aa168b21c064713b9883fe;n/a;-25dBm;2020-05-07 09:32:11",
Load Balancing	"radio1;c78236b5fb56b9023249e23e94dae7092aaa16f792aa168b21c064713b9883fe;n/a;-26dBm;2020-05-07 09:32:12", "radio1;f90a65957f2614491cc72284db4689020b2dbca102a237d0e94c10b7445cb4a4;n/a;-16dBm;2020-05-07 09:32:27",
System	<pre>"radio1;c78236b5fb56b9023249e23e94dae7092aaa16f792aa168b21c064713b9883fe;n/a;-25dBm;2020-05-07 09:32:45", "radio1;c78236b5fb56b9023249e23e94dae7092aaa16f792aa168b21c064713b9883fe;n/a;-26dBm;2020-05-07 09:32:46",</pre>
VPN	"radio1;f90a65957f2614491cc72284db4689020b2dbca102a237d0e94c10b7445cb4a4;n/a;-13dBm;2020-05-07 09:33:01", "radio1;c78236b5fb56b9023249e23e94dae7092aaa16f792aa168b21c064713b9883fe;n/a;-23dBm;2020-05-07 09:33:19",
	"radio1;c78236b5fb56b9023249e23e94dae7092aaa16f792aa168b21c064713b9883fe;n/a;-23dBm;2020-05-07 09:33:20",
Services	"radio1;f90a65957f2614491cc72284db4689020b2dbca102a237d0e94c10b7445cb4a4;n/a;-11dBm;2020-05-07 09:33:36", "radio1;c78236b5fb56b9023249e23e94dae7092aaa16f792aa168b21c064713b9883fe;n/a;-29dBm;2020-05-07 09:33:54",
Network	}
Statistics	

6.1.2.12 Rogue Access Point Detection Service

This service is used to detect unauthorized Access Points nearby and scans nearby access points and classifies them as "rogue" or "not rogue". The rogue APs are reported via SNMP traps.

Important

The rogue AP detection algorithm relies on the 8 THE FLYING CONTROLLER MECHANISM. The detection algorithm is only active on devices running in **controller** mode. As the controller mode selection is done automatically between devices running in the same network (LAN), all potentially candidates for Rogue AP detection have to be configured identically.

Multiple devices can take part on rogue access point detection. Every device running the AP scanning service and Flying Controller services and connected to the common wired network can be used as a part of the detection network. All scanned data from detection participants are requested by the controller device via SNMP calls and used for rogue AP detection.

Important

The rogue AP detection algorithm relies on the 6.1.2.10 Access Point Scanning Service (Wireless Monitoring) running on all participating devices.

As long as an SSID filter is enabled, only entries matching the predefined filter will be used during for detection. Known authorized devices can be whitelisted by using of whitelist parameter. Participants of the common network (i.e. the workers of the flying controller mechanism) are whitelisted automatically.

Important

System load and network traffic caused by SNMP calls can be minimized by using of SSID filter parameters. This also can be done for AP Scanner Service.

Participants connected to the wired network (all workers and the controller itself) are automatically whitelisted by service and not recognized as rogue devices. All other scanned APs with the same SSID will be declared as rogue and reported to a specified host. These notifications can be enabled with parameter "Enable SNMP Traps". IP address of the SNMP trap receiver can be configured with the parameter "Target address."

Status	Rogue AP Detection			
System VPN	Settings			
Services	Enable			
Customize	Activate SSID Filter	enable	•	
SNMPD	SSID Filter	vmn_i	×	
SNMPD Edit		SSID	+	
SNMP-Trap GPS Info	Whitelist	disable	-	
GPSD	Interval between detection cycles (seconds)	30		
Shadowsocks-libev	Enable SNMP-Traps			

Ø Specifies the server for SNMP-Traps

Save & Apply Save Reset

SNMP notifications are defined within the ELTEC MIB and have following format:

ELTEC-CYAP-MIB::rogueAPdetected ELTEC-CYAP-MIB::rogueDataSSID ELTEC-CYAP-MIB::rogueDataBSSID ELTEC-CYAP-MIB::rogueDataChannel ELTEC-CYAP-MIB::rogueDataSignal ELTEC-CYAP-MIB::rogueDataLastseen ELTEC-CYAP-MIB::rogueDataSISID

AP Scanner

OMR-Tracker

Rogue AP

Status messages can be discovered on the UI page (Status->RogueAP).

Status	Results
Overview	Mon Jan 11 11:44:27 2021 daemon.err uhttpd[9057]: luci: accepted login on /admin/status/rogueap for root from 192.168.100.180
Advanced	Mon Jan 11 11:44:31 2021 user.info rogueap: Starting up Mon Jan 11 11:44:31 2021 user.info rogueap: interval = 30 seconds.
Firewall	Mon Jan 11 11:44:31 2021 user.info rogueap: verbosity_level = 2
Routes	Mon Jan 11 11:44:31 2021 user.info rogueap: trap_enable = 1 Mon Jan 11 11:44:31 2021 user.info rogueap: target addr = 192.168.100.180
System Log	Mon Jan 11 11:44:31 2021 user.info rogueap: device state changed [unused]->[controller] Mon Jan 11 11:50:51 2021 user.info rogueap: detected S BSSID[00:15:61:20:AC:8A] SSID[vmn i] BSSID[C6:D7:31:3F:87:44] CHANNEL[1] SIGNAL[-45]
Kernel Log	Mon Jan 11 11:51:26 2021 user.info rogueap: detected s_BSSID[00:15:61:20:AC:8A] SSID[vmn_i] BSSID[C6:D7:31:3F:87:44] CHANNEL[1] SIGNAL[-45]
Processes	Mon Jan 11 11:51:26 2021 user.info rogueap: detected S_BSSID[00:15:61:20:AC:BA] SSID[vmn_i] BSSID[6A:74:22:9C:3C:8B] CHANNEL[1] SIGNAL[-41]
Realtime Graphs	
AP Scanner	
Rogue AP	

6.1.3 Multi-WAN Manager (MWAN3)

Important

Since MWAN3 and LinkAggregation are concurrent routing features, only one of them can be active at the same time. Please refer to chapter 6.1.4.1 OpenMPTCProuter versus MWAN3.

The multi-WAN manager (MWAN3) can be used to control which network connection is to be used for traffic. This section uses LTE uplink connections as example, but other connections - like WLAN or Ethernet - can also be used.

It provides the following features:

СҮВОХ АР З

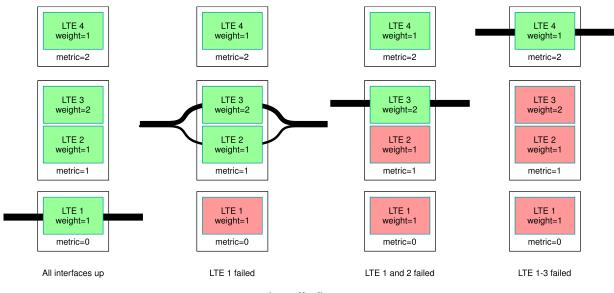
- Monitoring of WAN connectivity using repeated ping tests (ping | arping | httping).
- Routing of outbound traffic to another WAN interface if the first WAN interface loses connectivity, based on metric. The connection with the lowest metric is preferred, other connections are only used if the preferred one fails. Interfaces sharing the same metric value form a "group".
- Outbound WAN traffic load balancing over multiple WAN interfaces based on a numeric weight assignment. All connections sharing the same metric ("within the same group") are used simultaneously, distributing traffic over them. Connections with higher weights gets more traffic assigned.
- Different policies can be defined for different traffic types. For example, OpenVPN traffic could be routed through the first connection (using the other connections only if it fails), while routing all other traffic through the remaining connections (using load-balancing among them).

Load-balancing requires no remote station on the ground, it is handled entirely by the CyBox AP 3. As such, it is no link aggregation. It distributes traffic by streams, not by packets, i.e. a single stream cannot benefit from multiple LTE connections. For example, a single download stream can only use one LTE connection. However, multiple streams (e.g. generated by many WLAN users onboard a train) can be distributed over multiple WAN connections, increasing the overall bandwidth.

The figure Example traffic flow in MWAN shows an example configuration and visualizes the traffic flows in various situations:

- When all interfaces are up, all traffic is routed through the interface with the lowest metric, which is LTE 1 (metric=0).
- If LTE 1 fails, all traffic is still routed through the operable interfaces with the lowest metric (=1). But now, this is LTE 2 and LTE 3, which share the same metric. The traffic is distributed (load-balanced) over these interfaces.
- If LTE 1 and 2 fail, the traffic is routed over LTE 3, because this is now the operable interface with the lowest metric. There is no load-balancing any more, because only one interface is used.
- It LTE 1-3 fail, LTE 4 is used. Technically it is the operable interface with the lowest metric.

Note that the load balancing between LTE 2 and LTE 3 routes more traffic through LTE 3 than through LTE 2. This is because of the different weights. The interface with the higher weight gets more traffic. When there is now load balancing, the weight values have no effect.



Example traffic flow in MWAN

6.1.3.1 Capabilities

The MWAN3 package provides the following capabilities:

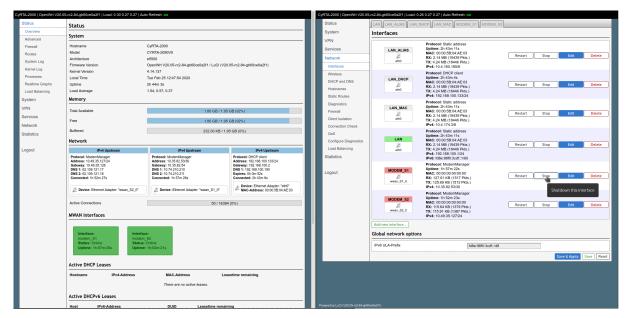
- provides outbound WAN traffic load balancing over multiple WAN interfaces based on a numeric weight assignment
- monitors WAN connections using repeated ping tests (ping | arping | httping) and automatically routes outbound traffic to another WAN interface if the first WAN interface loses connectivity
- provides specific outbound traffic rules to customize which outbound connections should use which WAN interface

6.1.3.2 MWAN Test

6.1.3.2.1 Gateway

After complete Modem setup the modem interfaces are up and tracking via ping is active. To check the hotplug MWAN mechanism open a second web interface to CyBox AP 3 and go to Network → Interfaces.

In this example MODEM_S1 has the lowest metric and will be first standard gateway. The test is started with *Stop* action on interface MODEM_S1.



MWAN test stopping a modem

As the interface is down, all traffic has stopped and standard gateway switches to modem 1.



yRTA-2000 OpenWrt V20.05	-rc2-84-gb60ce0a2f1 Load: 0.30 0.27 0.27 Au	to Refresh: on		CyRTA-2000 OpenWrt V20.0)5-rc2-84	gb60ce0a2f1 Load	1: 2.29 0.78 0.44 Auto Refresh: on	
Status	Status			Status	LAN	LAN_ALIAS LA	N_DHCP LAN_MAC MODEM_S1 MODE	M_52
Overview	System			System	Inte	erfaces		
Advanced	Hostname	CvRTA-2000		VPN			Protocol: Static address	
Firewall Routes	Model	CYRTA-2000		Services		LAN_ALIAS		
System Log	Architecture	e5500		Network		eth0	RX: 2.19 MB (19865 Pkts.) TX: 4.38 MB (19877 Pkts.)	Restart Stop Edit Delete
Kernel Log	Firmware Version		b60ce0a2f1 / LuCI (V20.05-rc2-84-gb60ce0a2f1)	Interfaces			IPv4: 10.4.160.185/8	
Processes	Kernel Version Local Time	4.14.137 Tue Feb 25 12:48:39 202	0	Wireless			Protocol: DHCP client Uptime: 2h 43m 51s	
Realtime Graphs	Uptime	2h 44m 48s		DHCP and DNS		LAN_DHCP	MAC: 00:00:5B:04:AE:03 RX: 2.19 MB (19865 Pkts.)	Restart Stop Edit Delete
Load Balancing	Load Average	2.12, 0.89, 0.49		Hostnames		eth0	TX: 4.38 MB (18877 Pkts.)	
System	Memory			Static Routes			IPv4: 192.168.100.133/24 Protocol: Static address	
VPN	Total Available		1.80 GB / 1.95 GB (92%)	Diagnostics		LAN_MAC	Uptime: 2h 43m 58s MAC: 00:00:58:04:AE:03	
Services				Client Isolation		eth0	RX: 2.19 MB (19865 Pkts.)	Restart Stop Edit Delete
Network	Free		1.80 GB / 1.95 GB (92%)	Connection Check			TX: 4.38 MB (18877 Pkts.) IPv4: 10.4.174.3/8	
Statistics	Buffered		232.00 KB / 1.95 GB (0%)	QoS			Protocol: Static address Uptime: 2h 43m 58s	
	Network			Configure Diagnostics		LAN	MAC: 00:00:5B:04:AE:03	
Logout	IPv4 Upstream	am IPv4 Upstream		Load Balancing		ett0	RX: 2.19 MB (19865 Pkts.) TX: 4.38 MB (18877 Pkts.)	Restart Stop Edit Delete
, in the second	Protocol: ModemManager		Protocol: DHCP client	Statistics			IPv4: 192.168.100.1/24 IPv6: fd8e:98f0:3cdf::1/60	
	Address: 10.49.35.127/24 Gateway: 10.49.35.128		Address: 192.168.100.133/24 Gateway: 192.168.100.2			MODEM_S1	Protocol: ModernManager RX: 0 B (0 Pkts.)	
	DNS 1: 62.109.121.17 DNS 2: 62.109.121.18		DNS 1: 192.168.100.190 Expires: 0h 0m 7s	Logout		wwan_S1_0	TX: 0 B (0 Pkts.)	Restart Connect Edit Delete
	Connected: 1h 53m 12s		Connected: 2h 43m 53s			www.cor_o	Information: Not started on boot Protocol: ModernManager	
	Device: Ethernet Adapter: "wwan_S2_0"		Device: Ethernet Adapter: "eth0" MAC-Address: 00:00:58:04:AE:03			MODEM_S2	Uptime: 1h 53m 10s MAC: 00:00:00:00:00 RX: 116.63 KB (1391 Pkts.)	
						wwan_S2_0		Restart Stop Edit Delete
	Active Connections		65 / 16384 (0%)			www.coz.o		
	MWAN Interfaces				Add	new interface		
				-	Glob	al network opti	ons	
	Interface: Interfac	Interface:						
	modem_S1 modem Status: Offine Status:			IPve	ULA-Prefix	fd8e:96f0:3cdf	/48	
	Downtime: Uptime						Save & Apply Save Reset	
	0h:0m:36s							
	Active DHCP Leases			-				
	Hostname IPv4-Address	MAC-Addres	s Leasetime remaining					
		There are no a	ctive leases.					
	Active DHCPv6 Leases							
		Powered by LuCI (V20.05-rc2-84-at						

MWAN test

6.1.3.3 MWAN Status

The detailed MultiWan status information is found in Status \rightarrow Load Balancing \rightarrow Detail.

Status	Interface Detail Diagnostics Troubleshooting
Overview	MWAN Status - Detail
Advanced	
Firewall	Interface status: interface modem S1 is offline and tracking is active
Routes	interface modem_S2 is online and tracking is active
System Log	Current ipv4 policies:
Kernel Log	balanced: modem S2 (100%)
Processes	modem_51_modem_52: modem_52 (100%)
Realtime Graphs	modem_S1_only:
Load Balancing	unreachable modem S2 modem S1:
System	modem S2 (100%)
VPN	modem_52_only: modem_52 (100%)
	Current ipv6 policies:
Services	balanced:
Network	unreachable modem S1 modem S2:
Statistics	unreachable
	modem_S1_only: unreachable
Logout	modem_S2_modem_S1: unreachable
Ŭ	modem_S2_only:
	unreachable
	Directly connected ipv4 networks:
	192.168.100.255 10.35.82.53
	127.0.0.0
	192.168.100.133 10.49.35.0/24
	192.168.100.1 10.49.35.255
	10.0.0.0/8
	10.49.35.0 10.0.0.0
	192.168.100.0
	192.168.100.0/24 10.35.82.55
	10.255.255.255
	10.4.174.3 10.35.82.52/30
	10.35.82.52
	127.0.0.1 224.0.0.0/3
	127.255.255.255
	10.4.160.185 10.49.35.127
	127.0.0.0/8
	Directly connected ipv6 networks:
	fd8e:98f0:3cdf::/64

MWAN detailed status page

6.1.3.4 MWAN Modem Interface Configuration

The MWAN interface configuration has a default setup for every modem card.

CONFIGURATION	

Status	Globale	nterfaces	Members D	olicies Rules	Notification						
System		obals Interfaces Members Policies Rules Notification									
VPN	There are co	re are currently 2 of 60 supported interfaces configured									
Services					e in the main rou	ting table					
Network			252 physical and/ l interfaces have a		s nfigured in /etc/con	fig/network					
Interfaces			interface name fo aracters A-Z, a-z,			2					
Wireless					embers, policies or	rules					
DHCP and DNS	Name	Enabled	Tracking method	Tracking method	Tracking reliability	Ping interval	Interface down	Interface up	Metric		
Hostnames	madam 61	Vac		Incurva	1	55	3	8	10	Edit	Delete
Static Routes	modem_S1		ping	_							
Diagnostics	modem_S2	Yes	ping	-	1	5s	3	8	20	Edit	Delete
Firewall			Add								
Client Isolation								Save &	Apply	Save	Reset
Connection Check											
QoS											
Configure Diagnostics											
Load Balancing											
Statistics											
Logout											

MWAN Interface configuration

The tracking parameters can handle target host IPs, ping interval and timeout.

Status	Globals Interfaces Members Policies	Rules Notification						
System	MWAN Interface Configuration	n - modem_S1						
VPN								
Services	Enabled							
Network	Initial state	Online _						
Interfaces	4	Expect interface state on up event						
Wireless	Internet Protocol	IPv4 •						
DHCP and DNS		IFV4						
Hostnames	Tracking hostname or IP address	8.8.8						
Static Routes		208.67.220.220 ×						
Diagnostics		+						
Firewall Client Isolation		Of this hostname or IP address will be pinged to determine if the link is up or down. Leave blank to assume interface is always online						
Connection Check	Tracking method	ping -						
QoS	Tracking reliability	1						
Configure Diagnostics								
Load Balancing		Acceptable values: 1-100. This many Tracking IP addresses must respond for the link to be deemed up						
Statistics	Ping count	1 💌						
Logout	Ping size	56 🗸						
	Max TTL	60 _						
	Check link quality							
	Ping size	56 _▼						
	Ping timeout	2 seconds 🔹						
	Ping interval	5 seconds -						
	Failure interval	5 seconds						
		Ping interval during failure detection						
	Keep failure interval							
		Keep ping failure interval during failure state						
	Recovery interval	5 seconds						
		Ping interval during failure recovering						
	Interface down	3 -						
		Interface will be deemed down after this many failed ping tests						
	Interface un							

Tracking parameters

6.1.3.5 MWAN Members Configuration

Members are profiles attaching a metric and weight to an MWAN interface. Names may contain characters A-Z, a-z, 0-9, _ and no spaces. Members may not share the same name as configured interfaces, policies or rules.

Status	Globals Interfaces Mem	bers Policies Rules	Notification]				
System	MWAN - Members		_					
VPN	Members are profiles attaching	a metric and weight to an	MWAN interfa	се				
Services	Names may contain characters Members may not share the sa	A-Z, a-z, 0-9, _ and no s	paces					
Network	Name	Interface	Metric	Weight				
Interfaces	modem_S1_m1_w3	modem_S1	1	3	Up	Down	Edit	Delete
Wireless	modem_S1_m2_w3	modem_S1	2	3	Up	Down	Edit	Delete
DHCP and DNS	modem_S2_m1_w2	modem_S2	1	2	Up	Down	Edit	Delete
Hostnames	modem_S2_m2_w2	modem_S2	2	2	Up	Down	Edit	Delete
Static Routes		Add						
Diagnostics						Save	& Apply	ave Reset
Firewall						Save	a Apply	Neset
Client Isolation Connection Check								
QoS								
Configure Diagnostics								
Load Balancing								
Statistics								
Statistics								
Logout								

MWAN members

6.1.3.6 MWAN Policies Configuration

Policies are profiles grouping one or more members controlling how MWAN distributes traffic. Member interfaces with lower metrics are used first. Interfaces with the same metric use load-balancing. Load-balanced member interfaces distribute more traffic out through those interfaces with higher weights.

Status	Globals Interfaces Members Policies Rules Notification							
System	MWAN - Policies							
VPN	Policies are profiles grouping one of		ow MWAN distributes traffic					
Services	Member interfaces with lower metrics are used first Member interfaces with the same metric will be load-balanced							
Network	Load-balanced member interfaces of Names may contain characters A-Z		e with higher weights					
Interfaces	Names must be 17 characters or les Policies may not share the same na		members or rules					
Wireless	Name	Members assigned	Last resort					
DHCP and DNS	modem_S1_only	modem_S1_m1_w3	unreachable (reject)	Up Down Edit Delete				
Hostnames Static Routes	modem_S2_only	modem_S2_m1_w2	unreachable (reject)	Up Down Edit Delete				
Diagnostics	balanced	modem_S1_m1_w3 modem_S2_m1_w2	unreachable (reject)	Up Down Edit Delete				
Firewall Client Isolation	modem_S1_modem_S2	modem_S1_m1_w3 modem_S2_m2_w2	unreachable (reject)	Up Down Edit Delete				
Connection Check	modem_S2_modem_S1	modem_S1_m2_w3 modem_S2_m1_w2	unreachable (reject)	Up Down Edit Delete				
QoS		dd						
Configure Diagnostics				Save & Apply Save Reset				
Load Balancing								
Statistics								
Logout								

MWAN policies page

6.1.3.7 MWAN Rules Configuration

Rules specify which traffic will use a particular MWAN policy based on IP address, port, or protocol. Rules are matched from top to bottom. Rules below a matching rule are ignored. Traffic not matching any rule is routed using the main routing table. Traffic destined for known (other than default) networks is handled by the main routing table. Traffic matching a rule, but with all WAN interfaces for that policy down, will be blackholed.

Status	Globals	nterfaces	bers Polici	es Rules Notifica	ation			
System	MWAN -	Rules						
VPN	Rules specify	y which traffic will	use a particula	ar MWAN policy				
Services		sed on IP address atched from top to		col				
Network	Rules below	a matching rule a	re ignored	the main routing table				
Interfaces				t) networks is handled is for that policy are do				
Wireless	Names may	contain characters	A-Z, a-z, 0-9	, and no spaces				
DHCP and DNS	Rules may n			figured interfaces, mer	•			
Hostnames	Name	Source address	Source port	Destination address	Destination port	Protocol	Policy assigned	
Static Routes	https	_	_	_	443	tcp	balanced	Up Down Edit Delete
Diagnostics	default_rule	e —	_	0.0.0/0	_	all	balanced	Up Down Edit Delete
Firewall	<i>i</i>							
Client Isolation			Add					
Connection Check								Save & Apply Save Reset
QoS								
Configure Diagnostics								
Load Balancing								
Statistics								
Logout								

MWAN rules page

6.1.3.8 MWAN Notification Configuration

In the advanced configuration you may add a custom specific action on MWAN3 hotplug events, on interfaces for which MWAN3 is enabled.

This section allows to modify the content of "/etc/mwan3.user". The file is also preserved during sysupgrade. Notes:

- This file is interpreted as a shell script.
- The first line of the script must be "#!/bin/sh" without quotes.
- Lines beginning with # are comments and are not executed.
- There are three main environment variables that are passed to this script:
- \$ACTION Either "ifup" or "ifdown"
- \$INTERFACE Name of the interface which went up or down (e.g. "wan" or "wwan")
- \$DEVICE Physical device name which interface went up or down (e.g. "eth0" or "wwan0")

Status	Globals Interfaces Members Policies Rules Notification
System	MWAN - Notification
VPN	This section allows you to modify the content of "/etc/mwan3.user".
Services	The file is also preserved during sysupgrade.
Network	Notes: This file is interpreted as a shell script.
Interfaces	The first line of the script must be "#!/bin/sh" without quotes.
Wireless	Lines beginning with # are comments and are not executed. Put your custom mwan3 action here, they will
DHCP and DNS	be executed with each netifd hotplug interface event
Hostnames	on interfaces for which mwan3 is enabled.
Static Routes	There are three main environment variables that are passed to this script.
Diagnostics	\$ACTION
Firewall	* "ifup" Is called by netifd and mwan3track * "ifdown" Is called by netifd and mwan3track
Client Isolation	 * "connected" Is only called by mwan3track if tracking was successful * "disconnected" Is only called by mwan3track if tracking has failed
Connection Check	\$INTERFACE Name of the interface which went up or down (e.g. "wan" or "wwan")
QoS	\$DEVICE Physical device name which interface went up or down (e.g. "eth0" or "wwan0")
Configure Diagnostics	#!/bin/sh
Load Balancing	<pre># # This file is interpreted as shell script.</pre>
	# Put your custom mwan3 action here, they will
Statistics	<pre># be executed with each netifd hotplug interface event # on interfaces for which mwan3 is enabled.</pre>
	<pre># # There are three main environment variables that are passed to this script.</pre>
Logout	# # \$ACTION
	# <ifup> Is called by netifd and mwan3track</ifup>
	# <ifdown> Is called by netifd and mwan3track # <connected> Is only called by mwan3track if tracking was successful</connected></ifdown>
	<pre># <disconnected> Is only called by mwan3track if tracking has failed # \$INTERFACE Name of the interface which went up or down (e.g. "wan" or "wwan")</disconnected></pre>
	# \$DEVICE Physical device name which interface went up or down (e.g. "eth0" or "wwan0")
	Submit Reset

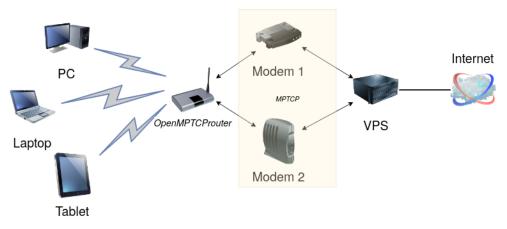
MWAN notification configuration

6.1.4 MultiPath TCP / Link Aggregation

Getting better throughput performance and failsave connections by using of MultiPath TCP (MPTCP) protocol. Link aggregation part is done by package OpenMPTCProuter.

OpenMPTCProuter

OpenMPTCProuter use MultiPath TCP (MPTCP) to really aggregate multiple Internet connections and OpenWrt.



A simple diagram to describe how OpenMPTCProuter is working.

Bonding connections to really aggregate bandwidth from up to 8 internet connections (Fiber, ADSL, VDSL, 4G,...) Provide hybrid Internet with any FAI

Failover

Always up with connection and VPS failover

Security

All data between the router and the VPS can be encrypted and obfuscated

Important

A **shall** precondition to use OpenMPTCProuter feature is the availability of at least two network interfaces e.g. modems configured and connected to provider. Otherwise no link aggregation or connection fallback will be possible.

6.1.4.1 OpenMPTCProuter versus MWAN3

MultiWAN (mwan3) algorithm distributes multiple TCP connections over multiple lines. All packets of one TCP session are always transferred over a single line. Resulting data throughput is limited by a capabilities of this line. In case of connection fail, established session will be closed. If other line is available, a new session will be established over another line.

While MultiWAN uses only one line for all session packets, OpenMPTCProuter split one TCP session over several lines. Resulting data throughput is limited by a sum of all used lines together. In case of a connection error e.g. one of a lines goes down, established session is not closed. Transmission of remaining TCP packets belonging to a session continues over other available lines.

6.1.4.2 OpenMPTCProuter/MWAN3 selection

OpenMPTCProuter and MWAN3 are concurrent tools and can not run at the same time. The active tool can be selected by using the UI page $S_{YStem} \rightarrow MWAN3$ and the command "routing_set mwan3" have to be executed. Also the factory reset is triggered. After the system restart MWAN3 UI pages and configuration defaults are available. OpenMPTCProuter UI pages and configurations are not available. To use OpenMPTCProuter instead of MWAN3 the same procedure has to be done. The only difference is using parameter "omr" instead of "mwan3" for command "routing_set".

CyBox(GW-P OpenWrt V20.29 Loa	ad: 0.41 0.31 0.23
	Status	Dashboard Configure
	System	Custom Commands
	System	
	Administration	System Information
	Startup	Command: cyap_status
	Scheduled Tasks	
	Mount Points	
	Backup / Flash Firmware	Run Download
	Custom Commands	
	License	ICCP Config
	Reboot	Command: cfg iccp
	VPN	Arguments:
	Services	
	Network	Run Download
	Statistics	
		Modem Gateway
	Logout	Command: modem_gateway
		Arguments:
		Run Download
		Select Routing App (!RESET ALL CONFIGURATIONS!)
		Command: routing_set
		Arguments: omr
		Run Download

6.1.4.3 VPS Configuration

6.1.4.3.1 Recommendations

Multiple interface data streams are ends up into a single data stream (Link Aggregation) on a special Server (VPS) which OpenMPTCProuter software are connecting to. Therefore the VPS/server need to have the lowest latency as possible with used network connections. It is recommended to use a linux based server with e.g. Debian 10 or Ubuntu 18.04 installed on as a VPS/server.

6.1.4.3.2 Install / setup VPS tools

VPS Setup is done by using of installation scripts provided by OpenMPTCProuter project.

Connect with SSH on your server, using ssh command under Linux or Putty under windows for example.

Then, as root:

wget -0 - https://www.openmptcprouter.com/server/debian10-x86_64.sh | sh

This will install and configure mptcp kernel, shadowsocks, glorytun and shorewall (as firewall). Key for shadowsocks and glorytun are generated by the script.

- SSH port is changed to 65222 (TCP)
- Shadowsocks port is 65101 (TCP & UDP)

- Glorytun port is 65001 (TCP & UDP)
- OMR JSON admin is 65500 (TCP)
- OpenVPN port is 65301 (TCP)
- MLVPN ports are 65201-65208 (UDP)
- Iperf3 on port 65400 (TCP & UDP)
- DSVPN port is 65401 (TCP)

6.1.4.3.3 Generated keys

After installation, keys can be found in file /root/openmptcprouter_config.txt.

```
root@fe-multipathtcp:# cat /root/openmptcprouter_config.txt
SSH port: 65222 (instead of port 22)
Shadowsocks port: 65101
Shadowsocks encryption: chacha20
Your shadowsocks key: xxxxxxxxxxxxxxxxxxxxxxxxxxx
Glorytun port: 65001
Glorytun encryption: chacha20
Your glorytun key: xxxxxxxxxxxxxxxxxxxxxxxx
A Dead Simple VPN port: 65011
A Dead Simple VPN key: xxxxxxxxxxxxxxxxxxxxxxxxxxx
MLVPN first port: 65201'
Your MLVPN password: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
Your OpenMPTCProuter Server key: xxxxxxxxxxxxxxxxxxxxxxxxxxxx
Your OpenMPTCProuter Server username: openmptcprouter
root@fe-multipathtcp:/home/eltec
```

6.1.4.3.4 Choosing a VPN Technology

Per default VPS (Virtual Private Server) is prepared to interact with multiple common implementations of VPN (Virtual Private Network) technology. Each of the supported VPN's OpenVPN/Glorytun/DSVPN/MLVPN) have preconfigured ports and keys. The decision which VPN should be used, or use it at all can be met by user during configuration of OMR (OpenMPTCProuter). The choice of using a VPN Shadowsocks only or a combination of Shadowsocks and VPN should be met depending on project goals and available tools.

Shadowsocks implementation make use of SOCKS5 Protocol which can handle not just multiple link connections, but also support different encryption methods. A default configuration of VPS and OMR software setup uses Shadowsocks connection for all TCP traffic and a GlorytunTCP VPN for any non-TCP traffic. In case Glorytun TCP VPN is deactivated or disconnected, all traffic is done over Shadowsocks interface. Alternative, if the Shadowsocks interface is disabled or disconnected, all data is send/received over Glorytun TCP VPN interface OMRVPN.

Important

In the following example, a default setup, a combination of Shadowsocks/Glorytun is used.

6.1.4.4 OpenMPTCProuter configuration example

The following example gives a step-by-step instruction of the configuration and testing of Link Aggregation with MPTCP by using two LTE modems as internet connections to a VPS server.

6.1.4.4.1 Setup DHCP

Optionally DHCP server functionality can be activated for LAN interface. This can be helpful for later connection of e.g. clients to router.

Status	LAN LAN_ALIAS LAN_DHCP LAN_MAC MODEM_S1 MODEM_S2 OMRVPN WAN1 WAN2 WAN6		
System	Interfaces - LAN		
VPN	On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use YLAN notation INTERFACE. VLANN (e.g., eth). 1).		
Services	Common Configuration		
Network	General Setup Advanced Settings Physical Settings Firewall Settings		
Interfaces	Status	Device: eth0	
Wireless DHCP and DNS Hostnames Static Routes Diagnostics		Uptime: IN 383 223 MAC: 0200 Stor 64 A02 274 C4.24 MB (14275 PMs.) TX: 0.24 MB (14275 PMs.) TX: 0.24 MB (1315 PMs.) PM+(151.08 10.03 274 PM+(56422 GMB0-100 PM+(56422 GMB0-100 PM+(56422 GMB0-100 PM+(56422 GMB0-100 PM+(56422 GMB0-100 PM+(56422 GMB0-100 PM+(56422 GMB0-100 PM+(5642 GMB0-	
Firewall	Protocol	Static address	
Client Isolation	Bring up on boot		
Connection Check MPTCP	IPv4 address	192.168.100.1	
QoS	IPv4 netmask	255.255.0 T	
Configure Diagnostics Statistics	IPv4 gateway		
Stausuus	IPv4 broadcast		
Logout	Use custom DNS servers	•	
	IPv6 assignment length	end e	
	IPv6 assignment hint	Assign prefix parts using this hexadecimal subprefix ID for this interface.	
	IPv6 suffix	-1	
		Optional. Allowed values: "cub4", 'anadom', fored value like 'L1' or 'L12". When IPv6 prefix (like 'a.bccd:') is received from a delegating server, use the suffix (like 'L1) to form the IPv6 address (adccd:1) for the interface.	
	DHCP Server		
	General Setup Advanced Settings IPv6 Settings		
	Ignore interface	Disable <u>DHCP</u> for this interface.	
	Start	100	
		Lowest leased address as offset from the network address.	
	Limit	150	
		Ø Maximum number of leased addresses.	
	Lease time	12h	
		Expiry time of leased addresses, minimum is 2 minutes (2m).	
	Back to Overview	Save & Apply Save Reset	

6.1.4.4.2 Remove / Disable unused default interfaces

Unused network interfaces should be either removed from configuration or set as disabled to not disturb MPTCP functionality.

CyBo	xGW-P OpenWrt V20.29 L	oad: 0.38 0.40 0.18 Auto Refresh: on						
	Status	LAN LAN_ALIAS LAN_DHCP LAN_	MAC MODEM_S1 MODEM_S2 OMRVPN WA	9.N6				
	System	Interfaces						
	VPN		Protocol: Static address					
	Services	LAN_ALIAS	MAC: 00:00:58:04:AD:02 RX: 120.91 KB (1021 Pkts.)		Restart	Connect	Edit	Delete
	Network	eth0	TX: 776.02 KB (1410 Pkts.) Information: Not started on boot					
	OpenMPTCProuter	LAN DHCP	Protocol: DHCP client MAC: 00:00:58:04:AD:02					
	Wireless	ethD	RX: 120.91 KB (1021 Pkts.) TX: 776.02 KB (1410 Pkts.) Information: Not started on boot		Restart	Connect	Edit	Delete
	DHCP and DNS	LAN_MAC	Protocol: Static address MAC: 00:00:58:04:AD:02					
	Hostnames Static Routes		RX: 120.91 KB (1021 Pkts.) TX: 776.02 KB (1410 Pkts.)		Restart	Connect	Edit	Delete
	Diagnostics	eth0	Information: Not started on boot					
	Firewall	LAN	Protocol: Static address Uptime: 0h 2m 49s					
	Client Isolation		MAC: 00:00:5B:04:AD:02 RX: 120.91 KB (1021 Pkts.)		Restart	Stop	Edit	Delete
	Connection Check MPTCP	eth0	TX: 776.02 KB (1410 Pkts.) IPv4: 192.168.100.1/24 IPv6: fd78:4c08:fbb1::1/60					
	QoS	OMRVPN	Protocol: DHCP client RX: 0 B (0 Pkts.)				Edit	Delete
	Configure Diagnostics Statistics	tun0	TX: 0 B (0 Pkts.) Error: Network device is not present		Restart	Stop	Edit	Delete
	Stausuus	MODEM_S1	Protocol: ModemManager RX: 0 B (0 Pkts.)					
	Logout	wwan_S1_0	TX: 0 B (0 Pkts.) Information: Not started on boot		Restart	Connect	Edit	Delete
		MODEM_S2	Protocol: ModemManager RX: 0 B (0 Pkts.)					
		www.sz_0	TX: 0 B (0 Pkts.) Information: Not started on boot		Restart	Connect	Edit	Delete
		WAN6	Protocol: DHCPv6 client					
		eth1	RX: 0 B (0 Pkts.) TX: 0 B (0 Pkts.) Information: Not started on boot		Restart	Connect	Edit	Delete
		Add new interface						
		Global network options						
		IPv6 ULA-Prefix		fd78:4c08:fbb1::/48				
							Sav	e & Apply Save Reset

6.1.4.4.3 Setup LTE Modems

Configuration of the first modem (MODEM_S1) can be done by using of UI page $Network \rightarrow Interfaces \rightarrow MODEM_S1$. In order to initiate a data connection, SIM_PIN and APN have to be specified. After that Bring up on boot flag has to be checked.

СуВа	ABoxGW-P OpenWrt V20 29 Load: 0 22 0.33 0.19 Auto Refresh: on				
	Status	LAN LAN_ALAS LAN_DHCP LAN_MAC MODEM_S1 MODEM_S2 MRVPN WANG			
	System	Interfaces - MODEM S1			
	VPN	On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge inter	rfaces" field and enter the names of sev	eral network interfaces separated by spaces. You can also use <u>VLAN</u> notation INTERFACE.VLANNR (e.g.: eth0.1).	_
	Services	Common Configuration			
	Network	General Setup Advanced Settings Physical Settings Firewall Settings			_
	OpenMPTCProuter	Status			
	Interfaces		Device: wwan_S1_0 RX: 0 B (0 Pkts.)		
	Wireless DHCP and DNS		TX: 0 B (0 Pkts.)		
	Hostnames	Protocol	ModernManager	Y	
	Static Routes	Bring up on boot	✓		
	Diagnostics	SIM card slot	Slot 1	•	
	Firewall Client Isolation	SIM Card Configuration			
	Connection Check	SIM Slot 1 SIM Slot 2 SIM Slot 3 SIM Slot 4			
	MPTCP	PIN	••••	*	
	QoS	APN	internet.telekom		
	Configure Diagnostics Statistics				
	Stausucs		Always use provider APN		
	Logout	Username		*	
		Password		*	
		Back to Overview		Save & Apply Save Re:	set

After applying new settings the connection process starts. After some time, depending e.g. on signal strength, modem connection should be established.

	Status	LAN LAN ALAS LAN DHCP LAN MAC MODEN SI MODEN SI MODEN SI MODEN SI MARINI WANK		
	System	Interfaces - MODEM_S1		
	VPN	Ch this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use VLAN notation INTERFACE. VLANIR (e.g.: ethel.).		
Services Common Configuration				
	Network	General Setun Advanced Settings Dhysical Settings		
	OpenMPTCProuter Interfaces	Status	Device: wwan S1 0	
	Wireless		Uptime: 0h 0m 155 MAC: 00:00:00:00:00	
	DHCP and DNS		EX: 168 B (2 Pkts.) TX: 720 B (8 Pkts.)	
	Hostnames		IPv4: 10.207.237.53/30	
	Static Routes Diagnostics	Protocol	ModernManager ·	
	Firewall	Bring up on boot	۲ ۲	
	Client Isolation	SIM card slot	Slot 1	
	Connection Check	SIM Card Configuration		
	QoS	SIM Slot 1 SIM Slot 2 SIM Slot 3 SIM Slot 4		
	Configure Diagnostics	PIN	*	
	Statistics	APN	Internet.telekom	
	Logout		Always use provider APN	
		Username	*	
		Password	*	
		Back to Overview	Save & Apply Save Reset	

Same procedure have to be done for the second modem interface (MODEM_S2) too.

CARO>	GW-P Openwit v20.29 Li	oad: 0.69 0.44 0.24 Auto Refresh: on		
	Status	LAN LAN_ALAS LAN_DHCP LAN_MAC WODEN_SI MODEN_SI OWRVPN WAND		
	System	Interfaces - MODEM_52		
	VPN	On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge inte	rfaces" field and enter the names of sever	al network interfaces separated by spaces. You can also use VLAN notation INTERFACE .VLANNR (e.g.: eth0.1).
	Services	Common Configuration		
	Network	General Setup Advanced Settings Physical Settings Firewall Settings		
	OpenMPTCProuter			
	Interfaces	Status	Device: wwan_S2_0 RX: 0 B (0 Pkts.)	
	Wireless		TX: 0 B (0 Pkts.)	
	DHCP and DNS Hostnames	Protocol	ModemManager	•
	Static Routes	Bring up on boot	×	
	Diagnostics	SIM card slot	Stot 1	•
	Firewall	SIM Card Configuration		
	Client Isolation Connection Check	SIM Slot 1 SIM Slot 2 SIM Slot 3 SIM Slot 4		
	MPTCP	PIN	••••	*
	QoS			<u>π</u>
	Configure Diagnostics	APN	internet.telekom	
	Statistics		Always use provider APN	
	Logout	Username		*
Ľ	Logour	Password		*
		Back to Overview		Save & Apply Save Reset

 CHU D 1 0 11/4 1/20 20 11 -	oad: 0.70 0.47 0.26 Auto Refresh: on		
	res we_dus_l we_dus_ wedus_l] wedus_l wedus_l webs_l wes		
VDN		rfaces" field and enter the names of several network interfaces separated by spaces. You can also use <u>VLAN</u> notation INTERFACE.VLANNR (e.g.: eth0.1).	
Senvices	Contrast page you can conligure the network interfaces. You can bridge several interfaces by locking the bridge inter Common Configuration	нають непо апо епісе пле наглез от земенат леммон плетнають зерагавер оу зрасез. Тоо сал аво озе <u>удоч</u> у поналогі ди селя не у осного до	
Network			
OpenMPTCProuter	General Setup Advanced Settings Physical Settings Firewall Settings		
Interfaces	Status	Device: wwan_S2_0 Uptime: 0h 0m 19s	
Wireless DHCP and DNS		AC: 00:00:00:00:00 RX: 890 B (9 Pkts.)	
Hostnames		TX: 19.11 KB (27 Pkts.) IPv4: 10.201.141.213/30	
Static Routes	Protocol	ModernManager •	
Diagnostics Firewall	Bring up on boot	v	
Client Isolation	SIM card slot	Slot 1	
Connection Check	SIM Card Configuration		
QoS	SIM Slot 1 SIM Slot 2 SIM Slot 3 SIM Slot 4		
Configure Diagnostics	PIN	**** *	
Statistics	APN	internet.telekom	
Logout		Ways use provider APN	
	Username	*	
	Password	*	
	Back to Overview	Save & Apply Save Reset	

6.1.4.4.4 Setup MPTCP

Now, MPTCP can be configured. This can be done by using of UI page ($Network \rightarrow MPTCP \rightarrow Settings$). By default MPTCP is enabled. Configuration of e.g. MultiPath TCP scheduler and MultiPath TCP path-manager can be done according to project goals. Configuration manual of a MultiPath TCP project ConfigureMPTCP contains further information about possible settings and their meaning.

GW-P OpenWitt V20.29 Load: 0.71 0.50 0.29				
Status Setting Bandwidth MPTCP Support Check MPTCP Fullmesh Established connections		ns		
System	мртср			
VPN	Networks MPTCP settings. Visit <u>http://multipath-tcp.org/unwiki.phpUsers/ConfigureMPTCP</u> for help.			
Services	GLOBALS			
Network	Multipath TCP	enable •		
OpenMPTCProuter Interfaces	Multipath TCP checksum	disable		
Wireless	Multipath Debug			
DHCP and DNS		disable •		
Hostnames	Multipath TCP path-manager	fullmesh		
Static Routes Diagnostics	Multipath TCP scheduler	default		
Firewall	Multipath TCP SYN retries	1		
Client Isolation	Congestion Control	bbr 👻		
Connection Check		Default is bor		
QoS	Fullmesh subflows for each pair of IP addresses	1		
Configure Diagnostics	Re-create fullmesh subflows after a timeout			
Statistics		enable 💌		
	ndiffports subflows number	1		
Logout	Interfaces Settings			
	LOOPBACK			
	Multipath TCP	disabled		
		One interface must be set as master		
	LAN			
	Multipath TCP	disabled 💌		
		One interface must be set as master		
	WAN6			

The role of each interface running MPTCP have to be defined. One interface have to be selected as master. Unused interfaces have to be marked as disabled.

WAN6	
Multipath TCP	disabled
	One interface must be set as master
OMRVPN	
Multipath TCP	disabled
	One interface must be set as master
LAN_ALIAS	
Multipath TCP	disabled
	One interface must be set as master
LAN_DHCP	
Multipath TCP	disabled
	One interface must be set as master
LAN_MAC	
Multipath TCP	disabled
	One Interface must be set as master
MODEM_S1	
Multipath TCP	master
	One interface must be set as master
MODEM_S2	
Multipath TCP	enabled
	One interface must be set as master
	Save & Apply Save Reset

6.1.4.4.5 Setup VPS access

Last part needed for using of Link Aggregation is configuration of OpenMPTCProuter (OMR). OMR configuration can be done by using of UI page (Network \rightarrow OpenMPTCProuter \rightarrow Settings Wizard). Server IP, username and also server key have to be entered.

CyBo	CyBoxGW-P OpenWin V20.29 Load: 0.20 0.36 0.27			
	Status	Settings Wizard Status Advanced Settings Show all settings		
	System	Wizard		
	VPN			
	Services	Server settings		
	Network			Delete
	OpenMPTCProuter	vps		
	Interfaces	Server IP	152.89.244.210	
	Wireless		Server IP will be set for ShadowSocks, Giorytun, OpenVPN and MLVPN	
	DHCP and DNS			
	Hostnames	Server username	openmptcprouter	
	Static Routes		② API username to retrieve personnalized settings from the server.	
	Diagnostics	Server key	/A7253F145AEC88B4E5C3699EA1B43254	
	Firewall		Key to configure and retrieve others keys from Server and to set server settings from OpenMPTCProuter.	
	Client Isolation			
	Connection Check MPTCP	Disable server		
	MPTCP OoS	Add server		

Settings according to technology which should be used for OMR<->VPS communication can be configured by using of the same UI page (Network > OpenMPTCProuter > Settings Wizard). Default setup allows usage of Shadowsocks between OMR and VPS. As a default encryption algorithm is chacha20 chosen. Also multiple different types of VPN endpoints can be used for communication between OMR and VPS.

Common server settings			
Advanced settings			
IPv6 settings			
Enable IPv6	You should disable IPv6 here if server doesn't provide IPv6.		
IPv6 ULA-Prefix	fd78:4c08:tbb1::/48 You can set a public IPv6 prefix only if you set only one server.		
ShadowSocks settings			
By default ShadowSocks is used for TCP traffic.			
ShadowSocks key	/eLtknOLzpP80ikNxV2bFtAzla++kDCUxrwC		
	Key is retrieved from server API by default. ShadowSocks is used for TCP.		
Disable ShadowSocks			
Encryption	chacha20 There is no Advanced Encryption Standard (AES) instruction set integrated in the processor, you should use chacha20. Encryption method is also used for Glorytun.		
VPN settings			
By default VPN is used for any traffic that is not TCP.			
Glorytun key	C03F164CAC99496058A02AF6287EED1B Key is retrieved from server API by default. Glorytun TCP is used by default for UDP and ICMP		
Default VPN	Glorytun TCP Set the default VPN used for UDP and ICMP when ShadowSocks is enabled, for all traffic if ShadowSocks is disabled. All VPN available here can do aggregation over MPTCP or using own internal method.		

Further network interface configuration according to OMR<->VPS communication can be done by using of the same UI page (Network → OpenMPTCProuter → Settings Wizard).

Interfaces settings				
You must disable DHCP on your moderns and set IP in different networks.				
modem_51	Delete			
Label				
	Q Label for the interface			
Protocol	Other •			
	O You can use DHCP if you have multiple real ethernet ports. Select other if you want to use another protocol available in Network Interfaces page.			
MPTCP over VPN				
	You can enable MPTCP over VPN if your provider filter Multipath TCP.			
Enable SQM				
	You should disable SQM for LTE or any interfaces with variable speed.			
Download speed (Kb/s)	٥			
	Used by Glorytun UDP and SQM/QoS if enabled. 0 to use default value.			
Upload speed (Kb/s)	0			
	© Used by Glorytun UDP and SQM/QoS if enabled. 0 to use default value.			
	Delete			
modem_S2	Delete			
inodem_52				
Label				
	Label for the interface			
Protocol	Other ·			
	O You can use DHCP if you have multiple real ethernet ports. Select other if you want to use another protocol available in Network Interfaces page.			
MPTCP over VPN				
	Ou can enable MPTCP over VPN if your provider filter Multipath TCP.			
Enable SQM				
	You should disable SQM for LTE or any interfaces with variable speed.			
Download speed (Kb/s)	٥			
	Used by Glorytun UDP and SQM/QoS if enabled. 0 to use default value.			
Upload speed (Kb/s)	0			
	Used by Glorytun UDP and SQM/QoS1 enabled. 0 to use default value.			
eth0 • Add an interface				
Select the device you want to base the interface on.				
The second and device you main to state the interface on.	Save & Apply Reset			

Advanced settings such as e.g. runtime Master interface selection can be done by using of UI page (Network \rightarrow OpenMPTCProuter \rightarrow Advanced Settings).

oxGW-P OpenWrt V20.29 Lo	ad: 0.77 0.53 0.35	
Status	Settings Wizard Status Advanced Settings Show all settings	
System	Advanced Settings	
VPN		
Services	VPS settings	
Network	vps	
OpenMPTCProuter	Redirects all ports from server to this router	
Interfaces	Disable ports redirection defined in firewall from server to this router	
Wireless DHCP and DNS	Networks settings	
Hostnames	IPv4 TCP Keepalive time	7200
Static Routes Diagnostics		
Firewall	IPv4 TCP FIN timeout	60
Client Isolation	IPv4 TCP SYN retries	3
Connection Check	IPv4 TCP Fast Open	3
MPTCP	Enable IPv6	
QoS Configure Diagnostics	Disable external check	When enable check are done on external sites to get each WAN IP and the IP used to go outside.
Statistics Logout	Disable TCP Fast Open	Disable TCP Fast Open on Linux and Shadowsocks configuration
Logon	Enable TCP Low Latency	Optimize for latency instead of bandwidth
		Save vnstats statistics on disk
	Disable gateway ping	Ocable gateway ping status check
	Disable default gateway	Disable default gateway, no internet if VPS are down
	Disable server ping	Disable server ping status check
	Master interface selection	Balancing
		Save & Apply Reset

After all settings are done and applied, network overview can be discovered by using of UI page (Network \rightarrow OpenMPTCProuter \rightarrow Status).

	enwit v20.25 [1	Load: 0.91 0.58 0.41 Auto Refresh: on	
Status		Settings Wizard Status Advanced Settings Show all settings	
System		Network overview	
VPN			
Services			
Network		VMN-ELTEC (192.168.100.241)	
OpenMPT	rcProuter		
Interfaces	3		
Wireless			
DHCP and			
Hostname			
Static Rou			
Diagnosti Firewall	CS .	CUR-UCINI D (102 100 100 1)	(()) modem_S1 (10.207.237.54) ip address: 10.207.237.53
Client Isol	lation	CyBoxGW-P (192.168.100.1)	wan address: 80.187.xxxxxx
Connectio	on Check	Load: 0.63 0.56 0.41	vhols: DTAG Internet service provider operations
MPTCP		Uptime: 0h 24m 10s Lan address: 192.168.100.1	latency: 43 ms mtu: 1500
QoS		Lan range: 192.168.100.100 - 192.168.100.249	operator: Telekom.de state: connected
Configure	Diagnostics		multipath: on
Statistics			
			(()) modem_S2 (10.201.141.214) <i>modem_S2</i> (10.201.141.214)
Logout			v van address: 80.1871.Jococox vhois: DTAG Internet service provider
			operations latency.22 ms
		cloud610967.fastpipe.io	mtu: 1496 operator. Telekom.de
		(152.89.2xxxxx) Version 0.1015 4.19.104-mptcp	state: connected multipath: on
		Load: 0.30 0.30 0.18	
		•••• Uptime: 4d 19h 14m 55s	
		Settings	
		Settings	
		Anonymize public IPs	₩

6.1.4.4.6 Speed test / IP

Previously configured OMR<-->VPS constellation is used to validate link aggregation functionality.

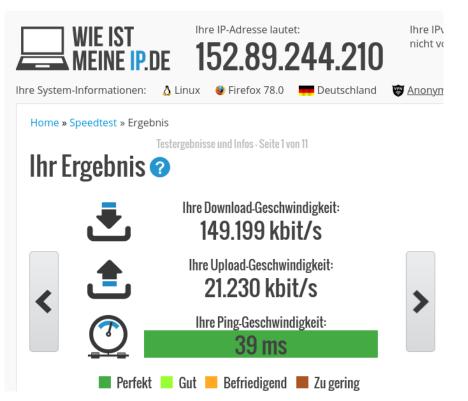
Important

Client connection to the internet destinations should be established over external VPS servers IP and not over one of two local uplinks at OMR! Check the IP reported by the website. It should match the IP of the VPS.

ELTEC systems

Important

Measured bandwidth is strongly dependent as well on currently available signal strength respectively quality as on contractual provider limitations for each used interface. Measurement values are only a snapshot. The exactly reproducibility can not be guaranteed!



6.1.5 LACP / Bonding

Getting better overall bandwidth and failsave connections by using of Link Aggregation Control Protocol (LACP).

Combining multiple Gigabit Ethernet interfaces into a single logical bonding interface results in increased overall bandwidth between connected devices.

For detailed information about bonding interface configuration parameter please refer to Linux Kernel documentation.

6.1.5.1 LACP configuration example

Following example gives a step-by-step instructions of configuration and testing of LACP with two Gigabit Ethernet devices.

Important

Please use a different interface for communication with the user interface than the one you want to use for LACP.

6.1.5.1.1 Create LACP interface

First of all a logical bonding interface should be created. This can be done by using of UI page (Network \rightarrow Interfaces \rightarrow Add new interface).

Add new interface	
Name	b1
Protocol	Link Aggregation (Channel Bonding)
	Cancel Create interface

6.1.5.1.2 Setup IP / Netmask

Next step is setting an ip address and a netmask for new created bonding interface (see tab -> General Settings).

Interfaces » B	1		
General Settings	Advanced Settings	Firewall Settings	
Status		Device: bonding-b1 RX: 0 B (0 Pkts.) TX: 0 B (0 Pkts.)	
Protocol		Link Aggregation (Channel Bond	ing) -
Bring up on boot			
IPv4 address		192.168.100.182	
		The local IPv4 address	
IPv4 netmask		255.255.255.0	_
		The local IPv4 netmask	
			Dismiss Save

6.1.5.1.3 Setup bonding Policy / add slave Interfaces

Slave interfaces and bonding policy (IEEE 802.3ad = LACP) can be configured with tab Advanced Settings.

General Settings Advanced Setting	Js Firewall Settings
Use builtin IPv6-management	
Force link	 Set interface properties regardless of the link carrier (If set, carrier sense events do not invoke hotplug handlers).
Slave Interfaces	eth0 eth1 v Image: Specifies which slave interfaces should be attached to this bonding interface v v
Bonding Policy	IEEE 802.3ad Dynamic link aggregation (Specifies the mode to be used for this bonding interface
Minimum Number of Links	0 Specifies the minimum number of links that must be active before asserting carrier
System Priority	65535 Specifies the system priority
MAC Address For The Actor	Specifies the mac-address for the actor in protocol packet exchanges (LACPDUs). If empty, masters' mac address defaults to system default
Aggregation Selection Logic	Aggregator: All slaves down or has no sla Specifies the aggregation selection logic to use
LACPDU Packets	Every 30 seconds (slow, 0) Specifies the rate in which the link partner will be asked to transmit LACPDU packets
Drop Duplicate Frames	Yes Specifies that duplicate frames (received on inactive ports) should be dropped or delivered
Link Monitoring	Off Method of link monitoring

6.1.5.1.4 Setup Firewall

If needed, firewall configuration can be done with tab Firewall Settings.

Interfaces » B1					
General Settings	Advanced Settings	Firewall Settings			
Create / Assign firewall-zone		unspecified	<u>•</u>		
		unspecified	ign to this		
		lan lan: 🗾	e interface stom field face to it.		
		vpn (empty)			
		wan (empty)	niss Save		
		custom			

6.1.5.1.5 Check interface Status

After applying new configuration settings, bonding interface bonding-b1 should be up and running.

	Protocol: Link Aggregation (Channel Bonding)
B1	Uptime: 0h 0m 31s
	MAC: 00:00:5B:03:B4:F8
2	RX: 29.20 KB (259 Pkts.)
bonding-b1	TX: 145.13 KB (288 Pkts.)
	IPv4: 192.168.100.182/24

Interface status can also be verified by using of debug console.

```
root@LACP_TEST:~# cat /proc/net/bonding/bonding-b1
Ethernet Channel Bonding Driver: v3.7.1 (April 27, 2011)
Bonding Mode: IEEE 802.3ad Dynamic link aggregation
Transmit Hash Policy: layer2 (0)
MII Status: up
MII Polling Interval (ms): 100
Up Delay (ms): 0
Down Delay (ms): 0
802.3ad info
LACP rate: slow
Min links: 0
Aggregator selection policy (ad_select): stable
System priority: 65535
System MAC address: 00:00:5b:03:b4:f8
Active Aggregator Info:
   Aggregator ID: 2
   Number of ports: 2
   Actor Key: 9
   Partner Key: 1
   Partner Mac Address: 44:a5:6e:43:5d:70
Slave Interface: eth0
MII Status: up
Speed: 1000 Mbps
Duplex: full
Link Failure Count: 1
Permanent HW addr: 00:00:5b:03:b4:f8
Slave queue ID: 0
Aggregator ID: 2
Actor Churn State: monitoring
Partner Churn State: monitoring
Actor Churned Count: 1
Partner Churned Count: 1
details actor lacp pdu:
  system priority: 65535
   system mac address: 00:00:5b:03:b4:f8
```

systems

```
port key: 9
   port priority: 255
   port number: 1
   port state: 61
details partner lacp pdu:
   system priority: 32768
   system mac address: 44:a5:6e:43:5d:70
   oper key: 1
   port priority: 128
   port number: 2
   port state: 63
Slave Interface: eth1
MII Status: up
Speed: 1000 Mbps
Duplex: full
Link Failure Count: 1
Permanent HW addr: 00:00:5b:03:b4:f9
Slave queue ID: 0
Aggregator ID: 2
Actor Churn State: monitoring
Partner Churn State: monitoring
Actor Churned Count: 0
Partner Churned Count: 1
details actor lacp pdu:
   system priority: 65535
   system mac address: 00:00:5b:03:b4:f8
   port key: 9
   port priority: 255
   port number: 2
    port state: 61
details partner lacp pdu:
   system priority: 32768
   system mac address: 44:a5:6e:43:5d:70
   oper key: 1
   port priority: 128
   port number: 1
    port state: 63
root@LACP_TEST:~#
```

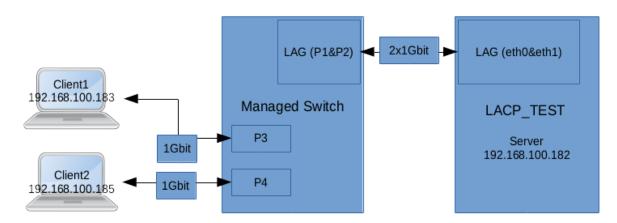
6.1.5.2 LACP testing example

After bonding interface is configured and running, additional hardware is needed for verification of its functionality.

One of the most common bonding usage scenarios is a improvement of bandwidth and reliability between Server and Client's.

6.1.5.2.1 Test Setup

To have a practical setup a managed Switch with LACP support, our previously configured LACP_TEST device and also two client PCs with 1 Gigabit Ethernet interface are needed.



6.1.5.2.2 Test bonding bandwidth improvement

Without using of logical bonding interface maximal available bandwidth between switch and LACP_TEST device would be 1 Gbit, from a purely theoretical point of view. So the client PC's which are connected to switch would share this bandwidth and get not more than 500Mbits each. As we configured two 1 Gigabit Ethernet devices to one logical bonding interface the maximal bandwidth should be 2 Gbit. Each Client should be abble to communicate with Server with maximal bandwidth of 1000Mbits.

In practical terms, the theoretical possible bandwidth cannot be reached! The maximal bandwidth would be round about 50-60% more than without bonding, so not 100%!

As a Measurement tool iperf is used. LACP_TEST device have iperf server instance running. Both client PC's communicating with the iperf server instance on LACP_TEST device at the same time. During the test we see both slaves of LACP_TEST bonding interface running. Each client communicates with the servers iperf instance over one of the both slave interfaces with about 800Mbits bandwidth.

6.1.5.2.3 Test bonding reliability improvement

In case Switch<->Server connection run without LACP, any communication errors will result in broken client connection. Due to reliability improvements of bonding implementation, communication between clients and server works also if one of the both LACP slaves goes down. This scenario can be easily verified by disconnecting one of the two bonding slaves e.g. eth0.

6.1.6 Global DHCP and DNS Settings

Be sure you understand DHCP and DNS services before changing any configurations. Under normal circumstances, keeping the factory default setting should be sufficient.

The CyBox AP 3 uses a DNS, TFTP and DHCP server. It is intended to provide coupled DNS and DHCP service to a LAN. This service accepts DNS queries and either answers them from a small, local, cache or forwards them to a real, recursive DNS server. See Chapter DHCP server 6.1.1.1 DHCP Server per Interface .

The DHCP server supports static address assignments and multiple networks. It automatically sends a sensible default set of DHCP options, and can be configured to send any desired set of DHCP options, including vendor-encapsulated options. It includes a secure, read-only, TFTP server to allow net/PXE boot of DHCP hosts and also supports BOOTP.

votom				
System	Dismasq is a combined <u>DHCP</u> -Server and <u>DNS</u> -Forwarder for <u>NAT</u> firewalls			
/PN	Server Settings			
Services				
letwork	General Settings Resolv and Hos			
Interfaces	Domain required	Don't forward <u>DNS</u> -Requests without <u>DNS</u> -Name		
Wireless				
HCP and DNS	Authoritative			
lostnames		This is the only <u>DHCP</u> in the local network		
Static Routes	Local server	/lan/		
Diagnostics		Local domain specification. Names matching this domain are never forwarded and are resolved from DHCP or hosts files only		
Firewall		-		
Client Isolation	Local domain			
Connection Check		Local domain suffix appended to DHCP names and hosts file entries		
QoS Configure Diagnostics	Log queries			
oad Balancing		Write received DNS requests to syslog		
atistics	DNS forwardings	/example.org/10.1.2.3 +		
latistics		List of <u>DNS</u> servers to forward requests to		
ogout	Rebind protection			
		Discard upstream RFC1918 responses		
	Allow localhost			
		Allow upstream responses in the 127.0.0.0/8 range, e.g. for RBL services		
	Domain whitelist	ihost.netflix.com +		
		② List of domains to allow RFC1918 responses for		
	Local Service Only			
		Limit DNS service to subnets interfaces on which we are serving DNS.		
	Non-wildcard			
		Bind dynamically to interfaces rather than wildcard address (recommended as linux default)		
	Listen Interfaces	+		
		Limit listening to these interfaces, and loopback.		
	Exclude interfaces	+		
		Prevent listening on these interfaces.		
		Save & Apply Save Reset		

DHCP And DNS Configuration Screen

6.1.7 Firewall

Be sure you understand zone-based firewalls before changing the firewall configurations.

The CyBox AP 3 has a built-in stateful firewall mapping interfaces into Zones that are used to describe default rules for a given interface, forwarding rules between interfaces, and extra rules that are not covered by the first two.

The first rule that matches is executed, often leading to another rule-chain until a packet hits either ACCEPT or DROP/REJECT. Such an outcome is final, therefore the default rules take effect last, and the most specific rule takes effect first. Zones are also used to configure masquerading also known as NAT (network-address-translation) as well as port forwarding rules, which are more generally known as redirects.

Zones must always be mapped onto one or more Interfaces, which ultimately map onto physical devices; therefore zones cannot be used to specify networks (subnets), and the generated iptables rules operate on interfaces exclusively. The difference is that interfaces can be used to reach destinations not part of their own subnet, when their subnet contains another gateway. Usually however, forwarding is done between LAN and WAN interfaces, with the router serving as 'edge' gateway to the Internet. The default configuration of the Firewall provides for such a common setup.

Status	General Settings Port Forwards Traffic Rules Custom Rules						
System	Firewall - Zone Settings						
VPN	The firewall creates zones over y	our network interface	es to control n	etwork traffic flo	w.		
Services	General Settings						
Network							
Interfaces	Enable SYN-flood protection						
Wireless	Drop invalid packets						
DHCP and DNS	Input		accept		-		
Hostnames	Output						
Static Routes			accept				
Diagnostics	Forward		reject	reject -			
Firewall	Routing/NAT Offloading						
Client Isolation	Experimental feature. Not fully con	patible with QoS/SQM	4.				
Connection Check							
QoS	Software flow offloading Software based offloading for routing/NAT						
Configure Diagnostics			U Soliwa	re based ollioad			
Load Balancing	Zones						
Statistics	Zone ⇒ Forwardings	Input Ou	tput	Forward	Masquerading		
	lan ⇒ wan	accept - ac	cept -	accept -	10	Ξ	Edit Delete
Logout	wan ⇒ REJECT	reject • ac	cept -	reject •] 🗹	Ξ	Edit Delete
	Add						
						Save & Apply	Save Reset

Firewall Zone Setting Screen

6.1.8 OpenVPN

Starting with firmware version 3.2 the Open Source VPN solution is included. The firmware before version 4.0 does not support a web frontend for OpenVPN configuration.

The OpenVPN program has many parameters to setup a connection. This chapter describes a basic Client OpenVPN tunnel configuration. In the next example the VPN tunnel connection is made through an already running LTE interface providing the Internet gateway.

6.1.8.1 Configuration file generation on Windows

OpenVPN for Windows can use an OpenVPN-GUI, which allows managing OpenVPN connections from a system tray applet. It can be used to generate a complete client configuration (zip file) including the .ovpn configuration file.

6.1.8.2 VPN interface setup – 3 methods

The VPN connection setup can be achieved by the three following methods.

6.1.8.2.1 Copy Ready-to-use configuration with SCP

This is the easiest way to configure a VPN connection. It is assumed that the server side has a configured network environment. The server administrator should create a valid client configuration package, including certificates, client keys and preferably a myclient.ovpn config file. The VPN connection is built on this configuration file (myclient.ovpn). This example uses four files that have to be static stored on the CyBox AP 3 to allow the openvpn

Delete

Delete

Delete

Upload

program to build up a connection without user interaction. If the 'auth-user-pass' option is given to openvpn without a parameter, the connection setup is interrupted and will ask for a username and password. To make this run automatically a two-line file with username (in first line) and password (in second line) has to be provided. All four files, the 'auth_user_pass', the 'pfelt1-udp-vpnuser_fg.p12' , the user key file 'pfelt1-udp-vpnuser_fg-tls.key' and the 'myclient.ovpn' config file have to copied from host system via 'scp' command to permanent storage located in '/etc/openvpn/' directory. Ensure that all files in '/etc/openvpn' have file permission 600 (cd /etc/openvpn; chmod 600 *).

The 'myclient.ovpn' configuration is:

dev tun persist-tun persist-key cipher AES-256-CBC auth SHA1
tls-client
client
resolv-retry infinite
remote 166.93.10.174 1194 udp
lport 0
verify-x509-name "VPN Server Cert" name
auth-user-pass auth_user_pass
pkcs12 pfelt1-udp-vpnuser_fg.p12
tls-auth pfelt1-udp-vpnuser_fg-tls.key 1
ns-cert-type server
comp-lzo

6.1.8.2.2 Upload configuration, certs, key-files with web interface

The second method is quite the same as the first. A modified 'myclient.ovpn' file is used. The difference is, that the certificate, the key files and the password files are uploaded from web interface. The default web interface upload directory is /etc/luci-uploads/ and the uploaded file is appended with service type and interface name e.g.:

/etc/luci-uploads/cbid.openvpn.my_vpn.myclient.ovpn

As a first step add your new VPN configuration using a predefinition.

1. New VPN configuration using a predefinition: Status OpenVPN System **OpenVPN** instances VPN Below is a list of configured OpenVPN instances and their current state Started Start/Stop Protocol Name Enabled Port **IPSecVPN** custom_config no start OpenVPN sample_server no start 1194 udp Services start sample_client no udp Network Template based configuration Statistics Instance name Select template ▼ Add OVPN configuration file upload Logout my_vpn Browse... pfelt1-udp-34447-vpnuser_fg.ovpn Save & Apply Save Reset

Edit your config.ovpn file and make sure that all certificates, key-files, user-name-pass files have the correct path including your config name, here 'my_vpn'.

The prepared 'myclient.ovpn' configuration looks like and is ready for upload:

(uploaded to /etc/luci-uploads/cbid.openvpn.my_vpn.myclient.ovpn)

```
dev tun
persist-tun
persist-key
cipher AES-256-CBC
auth SHA1
tls-client
client
resolv-retry infinite
remote 166.93.10.174 1194 udp
lport 0
verify-x509-name "VPN Server Cert" name
auth-user-pass
/etc/luci-uploads/cbid.openvpn.my\_vpn.auth\_user\_pass
pkcs12
/etc/luci-uploads/cbid.openvpn.my\_vpn.pfelt1-udp-vpnuser\_fg.p12
tls-auth
/etc/luci-uploads/cbid.openvpn.my\_vpn.pfelt1-udp-vpnuser\_fg-tls.key
1
ns-cert-type server
comp-lzo
```

6.1.8.2.3 Manual configuration with web interface

The third method does not use a preconfigured .ovpn file. You will have to enter each single parameter in the web interface. As the service is started, all given parameter are passed to the 'openvpn' program. This method may be useful for fast switching of parameters for server and client.

6.1.8.3 VPN host configuration (on console)

After the VPN client part configuration has been done, it's time to configure the rest of the system and start a first connection. This configuration can be done at console (via SSH) with 'uci' commands.

The openvpn program execution on the CyBox AP 3 is managed with the '/etc/init.d/openvpn' script.

The following configuration is done at the command prompt:

Create the VPN interface: (if not running server-bridge)

```
uci set network.vpn0=interface
uci set network.vpn0.ifname=tun0
uci set network.vpn0.proto=none
uci set network.vpn0.auto=1
```

Allow inbound VPN traffic:

```
uci add firewall rule
uci set firewall.@rule[-1].name=Allow-OpenVPN-Inbound
uci set firewall.@rule[-1].target=ACCEPT
uci set firewall.@rule[-1].src=\*
uci set firewall.@rule[-1].proto=udp
uci set
`firewall.@rule[-1].dest_port=1194 <mailto:firewall.@rule[-1].dest_port=1194>`_
```

Allow OpenVPN tunnel utilization: (not needed when bridging using tap)

```
uci set firewall.@zone[-1].input=REJECT
uci set firewall.@zone[-1].forward=REJECT
uci set firewall.@zone[-1].output=ACCEPT
uci set
`firewall.@zone[-1].network=vpn0 <mailto:firewall.@zone[-1].network=vpn0>`___
uci set firewall.@zone[-1].masq=1
uci set firewall.@zone[-1].mtu\_fix=1
uci add firewall forwarding
```

СҮВОХ АР З

ELTEC

```
uci set firewall.@forwarding[-1].src='lan'
uci set firewall.@forwarding[-1].dest='vpn'
```

Commit the changes:

```
uci commit network
/etc/init.d/network reload
uci commit firewall
/etc/init.d/firewall reload
```

Enable the start flag and setup configuration file:

```
echo > /etc/config/openvpn
uci set openvpn.vpn=openvpn
uci set openvpn.vpn.enabled=1
uci set openvpn.vpn.config='/etc/openvpn/myclient.ovpn'
uci commit openvpn
```

Finally do a first test and start manually the openvpn connection:

/etc/init.d/openvpn start

Use the 'logread' command to watch the connection progress.

```
Nov 26 15:59:05 CyBoxAP daemon.notice openvpn(vpn)[8040]: OpenVPN 2.3.4
powerpc-openwrt-linux-gnu [SSL (OpenSSL)] [LZO] [EPOLL] [MH] [IPv6]
built on Nov 12 2015
Nov 26 15:59:05 CyBoxAP daemon.notice openvpn(vpn)[8040]: library
versions: OpenSSL 1.0.1i 6 Aug 2014, LZO 2.08
Nov 26 15:59:06 CyBoxAP daemon.notice openvpn(vpn)[8040]: Control
Channel Authentication: using 'pfelt1-udp-vpnuser\_fg-tls.key' as a
OpenVPN static key file
Nov 26 15:59:06 CyBoxAP daemon.notice openvpn(vpn)[8040]: UDPv4 link
local (bound): [undef]
Nov 26 15:59:06 CyBoxAP daemon.notice openvpn(vpn)[8040]: UDPv4 link
remote: [AF\_INET] 166.93.10.174:1194
Nov 26 15:59:06 CyBoxAP daemon.warn openvpn(vpn)[8040]: WARNING: this
configuration may cache passwords in memory -- use the auth-nocache
option to prevent this
Nov 26 15:59:08 CyBoxAP daemon.notice openvpn(vpn)[8040]: [VPN Server
Cert] Peer Connection Initiated with [AF\_INET] 166.93.10.174:1194
Nov 26 15:59:11 CyBoxAP daemon.notice openvpn(vpn)[8040]: TUN/TAP device
tun0 opened
Nov 26 15:59:11 CyBoxAP daemon.notice openvpn(vpn)[8040]: do\_ifconfig,
tt->ipv6=0, tt->did\_ifconfig\_ipv6\_setup=0
Nov 26 15:59:11 CyBoxAP daemon.notice openvpn(vpn)[8040]: /usr/sbin/ip
link set dev tun0 up mtu 1500
Nov 26 15:59:11 CyBoxAP daemon.notice openvpn(vpn)[8040]: /usr/sbin/ip
addr add dev tun0 local 192.168.20.6 peer 192.168.20.5
Nov 26 15:59:11 CyBoxAP daemon.notice netifd: Interface 'vpn0' is
```

enabled

Nov 26 15:59:11 CyBoxAP daemon.notice netifd: Network device 'tun0' link is up Nov 26 15:59:11 CyBoxAP daemon.notice netifd: Interface 'vpn0' has link connectivity Nov 26 15:59:11 CyBoxAP daemon.notice netifd: Interface 'vpn0' is setting up now Nov 26 15:59:11 CyBoxAP daemon.notice netifd: Interface 'vpn0' is now up Nov 26 15:59:11 CyBoxAP daemon.notice openvpn(vpn)[8040]: Initialization Sequence Completed Nov 26 15:59:11 CyBoxAP user.notice firewall: Reloading firewall due to ifup of vpn0 (tun0

6.1.9 ICCP

The Inter **C**arriage **C**onnection **P**rotocol is a bridging algorithm developed by ELTEC to automatically establish and maintain a wireless LAN backbone for trains. It can be used in retrofit applications, where it is too expensive to install backbone Ethernet cables in throughout the train. The challenge is to establish and maintain connections in an unstable environment, exposed to disturbances, such as train re-configuration, connection losses, or other trains on neighbor tracks.

The main characteristics of ICCP are:

- Utilization of RSSI to determine best coupling partner in range
- Usage of WDS (Wireless Distribution System) mode for AP_Master-Client connection
- Support of all encryption modes (WPA2-PSK, etc.)
- One-Time configuration
- Unattended coupling/decoupling process, restore of previously established connections after power loss
- Free channel selection in 2.4 GHz with all HT-modes or 5 GHz with HT-modes (20/40/80)

6.1.9.1 Coupling Concept

The coupling concept follows different states in which the access point tries to determine the best partner for communication, establishes a connection and maintains it. The following table provides an overview of the states.

ICCP Coupling States:

State	Description
IDLE	The radio is enabled. The default mode is AP with SSID broadcasted and own serial number coded into the SSID. The WLAN mode is configured as "Access Point (WDS)" master using an eight character SSID broadcasted and own serial number coded into the SSID. The LAN port is configured for bridging and Spanning Tree Protocol is enabled.
BIND	WLAN has been enabled and the device searches for the qualified peer offering the best signal strength. The search is repeated multiple times to ensure that a stable situation is encountered. To qualify as best neighbor requires a minimal signal quality. The ID (foreign serial number) of the best neighbor found is passed to the next state CONNECT.

CONNECT	The own ID and the ID of the best neighbor found are coded into the new own SSID; the device waits for an SSID broadcast of the neighbor device with the same combination of IDs. This state has a time limit to establish the connection. If the time limit is exceeded, the state falls back to BIND. The expected client partner can extend the time limit for the master to set a common SSID, and switches into ESTABLISHED state as soon as the SSID contains the "EST" marker.
ESTABLISHED	Both devices enter a new configuration: the device with the larger ID becomes "Master" the other device becomes "Client". The SSID that has been negotiated in the previous state becomes hidden, if the master recognizes the client MAC. The WLAN access key is derived from the IDs.
DROPPED	Connection lost due to radio disturbance or train reconfiguration. The device tries to re-establish the last known connection for a preconfigurable time.

6.1.9.2 SSID Usage

The coupling procedure takes advantage of the fact that SSIDs contain alphanumeric characters and that it can be broadcast. Thus, an SSID can be used to broadcast information useful for coupling and enter a dialog to establish the connection. The access points will use their serial numbers - an eight-digit number - to identify themselves. In addition, the SSID may contain state information to allow the potential communication peer to monitor the progress of the negotiation. However, the current implementation does not use this additional state information. The SSIDs start with a well-known sequence of letters ("CyAP"), providing a means to filter out radio activities of other networks' access points. Starting with firmware version 4.0 this start tag "CyAP" is changeable but must keep its length of four characters.

The following table provides an overview of the SSIDs used in different states.

ICCP SSIDs Used:

SSID	Description
СуАРі_оооооооо	SSID broadcasted during BIND state. The characters ooooo are replaced by the own serial number of the AP. The letter 'i' represents the index of the WLAN module.
CyAPi_oooooooo_ nnnnnnnn	SSID broadcasted during CONNECT state. The characters ooooo are replaced by the own serial number of the AP, the characters nnnnn are replaced by the serial number of the AP that has been detected as best neighbor during search state.
CyAPi_oooooooo_ nnnnnnnn	SSID broadcasted at the begin of ESTABLISHED state. Still the same as in CONNECT, but only for a few seconds until the master detects the MAC link
CyAPi_oooooooo_ nnnnnnnn_ESTp	Private SSID (not broadcasted), used during state ESTABLISHED. Coding is identical to CONNECT SSID. The letter 'p' represents the index of the partner WLAN module.
CyAPi_oooooooo_ nnnnnnnn_ <custo m-ssid/network></custo 	VLAN mode only. Private SSID (not broadcasted), used during state ESTABLISHED. Coding is identical to CONNECT SSID.

6.1.9.3 WLAN Encryption

A suitable encryption mode must be activated for the communication between the wagons. For authentication individual access keys (PSK) must be established between the peers. The key is generated from the SSID using a hash algorithm that is known by both access points. During BIND and CONNECT state the WLAN mode is set to "Access Point (WDS)" (Wireless Distribution System), using an eight character random key for encryption.

6.1.9.4 Configurable Parameters

Before configuring the ICCP parameters, make sure that the following actions have been done:

- Delete all unnecessary interfaces with the web interface tab Network → Interfaces (e.g. *lan_alias*)
- Configure your ICCP management interface as desired in Network → Interfaces (e.g. configure the *lan* interface as a bridge composed of eth0, wlan0 and wlan1, then set the IP address to 192.168.100.2)
- Enable the WLAN radio you want to use for ICCP in $\underline{Network} \rightarrow WiFi$ (e.g. radio o only).

After that, you can start configuring ICCP in the tab 'Services' \rightarrow 'ICCP'. Then click 'Save & Apply'.

Status	Inter Carriage Connection Protocol	
System	ICCP provides automatic Wifi coupling between train carriages	
VPN	ICCP parameters for radio0	
Services	Enable protocol	
Customize SNMPD		Give ICCP exlusive usage on this radio
SNMPD Edit	Protocol mode	dynamic -
SNMP-Trap		
GPS Info		Wifi parameters are negotiated by partners (dynamic) or already applied for 'static' mode
GPSD ICCP	Debug ICCP	Enable more ICCP debug messages for 'Advanced Status' page
Softflowd	Tag name	CyAP
Network		
Statistics		Tag name string, length must be 4, unified among ICCP partners
Logout	Custom key extension	
		Custom key extension string: max.length 20, unified among ICCP partners
	Used vlan networks	
	VLAN tunnel	
		Use a tunnel to transfer VLAN tags, otherwise one wifi channel per VLAN network
	VLAN tunnel MTU	1500
		Use this MTU value for the tunnel device
	Min signal quality	-60
		Minimal signal quality (BIND threshold) [dBm]
	Quality check	0
		Orop ESTABLISHED if signal quality is lower than minimal for this time slot [sec] (0=disabled)
	Sustained discover	3
		Wumber of sustained discoveries as best partner in BIND/CONNECT phase
	Max Time	90
		Maximum CONNECT phase time [sec]
	Time extension	30
		CONNECT phase time extension [sec]
	Drop wait	10
		Wait [sec] before enter DROPPED state
	Drop retry	5
		In Number of retries to switch from DROPPED to ESTABLISHED state
	ICCP parameters for radio1	
	Enable protocol	0
		Give ICCP exlusive usage on this radio
		Save & Apply Save Reset

ICCP Configuration Screen

Note 1: When ICCP is used without VLAN connections, the 'dynamic' mode has to be used.

Note 2: 'Operating frequency parameters' must be identical for both ICCP partners.

Table 6 table below lists the parameters that influence the timing behavior or the connection procedure.

ELTEC systems

ICCP Parameters:

Parameter	Description	Unit	Range	Default
USED_VLAN_N ETWORKS	Using standard ICCP: empty - ICCP sets up a bridge between native eth0 and wlan0/1. Using VLAN ICCP: List of all configured VLAN networks/ssid. Case sensitive names for network interfaces and virtual SSIDs should configured first in appropriate menu pages.	Comma separated list	custom	empty
CHANNEL_SET TINGS	Predefined channel settings - make sure all desired coupling partners uses the same channel mode.	mode string	predefined or custom	2.4 GHz, CH 11, HT40-
MIN_SIGNAL_Q UALITY	Minimal signal quality. Partners below that value will be ignored.	dBm	-1000	-60
RECOVER	Number of times that another AP must be detected as best neighbor in a row. This value applies to BIND and CONNECT state.	times	15	3
CONNECT_MAX TIME	Time limit for connection state.	seconds	20200	90
CONNECT_EXT ENSION	Client time limit extension for connection state.	seconds	160	30
WAIT_RECONN ECT	Time to wait for reconnecting an established link (link signal lost).	seconds	330	10
DROPPED_RET RY	Value that determines the time in which the AP will attempt to re-connect the previous connection, using the stored SSID and access key. The old SSID and access key will be discarded if this time has elapsed, and the AP will enter IDLE state.	times	110	5

6.1.9.5 Configuration Hint Web Interface

When the ICCP process is enabled and configured on both partners, the protocol status can be observed via web interface on main status/advanced page ICCP menu tab.

\supset
<
0
\supset
(D)
0
<u></u>

Status	Module Information Revision Information Temperature Sensors GPS Sensors IICCP Self Test
Overview	ICCP Connection Progress
Advanced	THE REF / DUIDE-T/ EVEN DELTIDELE (JETUID) ELIV. EJROLENIED - HUSEL LINK LOSE
Firewall	Tue Apr 7 08:02:51 2020 user.notice [3150.25] ICCP0: ESTABLISHED : Master Link Lost Tue Apr 7 08:02:53 2020 user.notice [3152.31] ICCP0: ESTABLISHED : Master Link Lost
Routes	Tue Apr 7 08:02:55 2020 user.notice [3154.34] ICCP0: ESTABLISHED : Master link lost
System Log	Tue Apr 7 08:02:57 2020 user.notice [3156.39] ICCP0: ESTABLISHED : Master link lost Tue Apr 7 08:02:59 2020 user.notice [3158.41] ICCP0: ESTABLISHED : Master link lost
Kernel Log	Tue Apr 7 08:03:01 2020 user.notice [3160.44] ICCP0: ESTABLISHED : Master link lost Tue Apr 7 08:03:05 2020 user.notice [3164.58] ICCP0: ESTABLISHED : Master link lost
Processes	Tue Apr 7 08:03:07 2020 user.notice [3166.65] ICCP0: ESTABLISHED : Master Link lost Tue Apr 7 08:03:09 2020 user.notice [3168.08] LCCP0: ESTABLISHED : Master Link lost
Realtime Graphs	Tue Apr 7 08:03:11 2020 user.notice [3170.73] ICCP0: ESTABLISHED : Master link lost
Load Balancing	Tue Apr 7 08:03:13 2020 user.notice [3172.75] ICCP0: ESTABLISHED : Master link lost Tue Apr 7 08:03:15 2020 user.notice [3174.77] ICCP0: ESTABLISHED : Master link lost
System	Tue Apr 7 08:03:19 2020 user.notice [318.08] ICCP0: ESTABLISHED : Master Link lost Tue Apr 7 08:03:22 2020 user.notice [318.09] ICCP0: ESTABLISHED : Master Link lost
VPN	Tue Apr 7 08:03:24 2020 user.notice [3183.00] ICCP0: ESTABLISHED : Master Link lost Tue Apr 7 08:03:26 2020 user.notice [3185.06] ICCP0: ESTABLISHED : Master Link lost
Services	Tue Apr 7 08:03:28 2020 user.notice [3187.08] ICCP0: ESTABLISHED : Master link lost Tue Apr 7 08:03:30 2020 user.notice [3189.10] ICCP0: ESTABLISHED : Master link lost
Network	Tue Apr 7 08:03:34 2020 user.notice [3193.23] ICCP0: ESTABLISHED : Master link lost Tue Apr 7 08:03:36 2020 user.notice [3195.29] ICCP0: ESTABLISHED : Master link lost
Statistics	Tue Apr 7 08:03:39 2020 user.notice [3198.53] ICCP0: ESTABLISHED : Master link lost Tue Apr 7 08:03:41 2020 user.notice [3200.57] ICCP0: ESTABLISHED : Master link lost
	Tue Apr 7 08:03:43 2020 user.notice [3202.61] ICCP0: ESTABLISHED : Master link lost Tue Apr 7 08:03:45 2020 user.notice [3204.67] ICCP0: ESTABLISHED : Master link lost
Logout	Tue Apr 7 08:03:47 2020 user.notice [3206.71] ICCP0: ESTABLISHED : Master link lost Tue Apr 7 08:03:49 2020 user.notice [3208.73] ICCP0: ESTABLISHED : Master link lost
	Tue Apr 7 08:03:51 2020 user.notice [3210.87] ICCP0: ESTABLISHED : confirmed after 14 seconds - Hiding SSID; Saving Configuration. Tue Apr 7 08:04:04 2020 user.notice [3220.31] ICCP0: ESTABLISHED : Master link lost

ICCP Status Indication on Web Server

6.1.9.6 VLAN over Wireless ICCP

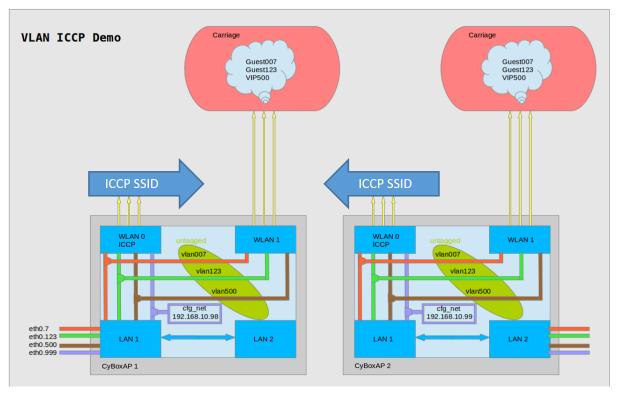
The latest ICCP implementation has been enhanced to be used in a VLAN network environment. This may increase network security by splitting the traffic into different virtual channels, i.e. a dedicated channel for the configuration and for service purposes as well as other channels, e.g. for guest access and VIP access.

6.1.9.6.1 Features and Restrictions

- The native 'eth0' interface and the native 'wlan0/1' (which is used by ICCP) are no longer available for any bridge devices.
- The backbone VLAN networks/bridges must be configured manually. Each VLAN channel needs a separate network interface.
- The network interface name can be up to 7 characters long. Any character may be used, but *name* must not be a substring of another name. e.g. a combination of 'vlan1' and 'vlan123' is not allowed. Names should be 'vlan001' and 'vlan123' instead.
- The corresponding Ethernet interface must be created (e.g eth0.123 for vlan123).
- All VLAN channels (network name) on the backbone must be exactly entered as a comma separated list in ICCP menu entry 'Used VLAN networks'.
- The second WLAN module, which is not used for ICCP, can act as standard Access Point. The SSIDs for this module must different from any name used as an ICCP SSID. Traffic on these Access Point SSIDs are always untagged, but will be tagged as soon as packets enter a backbone bridge. Any traffic on the backbone is tagged.
- As soon as the master channel is in established state, all configured 'Used VLAN networks' will be started via tunnels (i.e. gretap interfaces). After all channels are in established state, the configuration is permanently saved. Thus, the ICCP partners can quickly reconnect at the next power up of the system. If the connection drops and the master channel goes to idle state, the corresponding VLANs will be disabled.

6.1.9.6.2 Examples

Figure 34 shows an example of a configuration that uses VLANs over ICCP.



ICCP illustration for VLAN Usage

Case 1: Dynamic ICCP

The configuration has to be performed on both ICCP partners.

a. Interfaces configuration

In addition to the steps described in Configurable Parameters, each VLAN (vlan007 and vlan123) must be configured as follows:

- Create new interface called 'vlan007' in the tab $\texttt{Network} \rightarrow \texttt{Interfaces}$
- When ask to specify a physical interface, create the custom interface called '*eth0.007*' then click on Save & Apply
- b. ICCP VLAN configuration

ICCP can be configured via the web interface as shown below, or via the command line with the command 'cfg_iccp -d -p dynamic -r 0 -v vlan123 -v vlan007'.

Inter Carriage Connection Protocol System ItcP provide automatic Will coupling between train carriages Customize Customize Control Customize Customize <thcit customize<="" in="" ind="" is="" th="" thigh=""> <thcus< th=""><th></th></thcus<></thcit>		
VPN CCP parameters for radio0 Sorvices Enable protocol © isive ICCP extusive usage on this radio SNMPD Edit Protocol mode dynamic SNMP-Trap @ OP on this radio @ OP on this radio GPS Info @ OP on this radio @ OP on this radio GPS Info @ Debug ICCP @ Enable more ICCP debug messages for 'Advanced Status' page ICCP @ Enable more ICCP debug messages for 'Advanced Status' page Statistics Tag name CyAP Custom key extension @ Tag name string, length must be 4, unified among ICCP partners Custom key extension @ Custom key extension string: max.length 20, unified among ICCP partners Logout @ Lunnel @ Use a lunnel to transfer VLAN tags, otherwise one wifi channel per VLAN network VLAN tunnel @ Use this MTU value for the tunnel device @ Use this MTU value for the tunnel device Minimal signal quality		
Services Customize SIMIPD SimiPD Edit SiMIPD Edit SiMIPD Edit SiMIPD Trap GPS Info 		
SIMIPD Edit Protocol mode dynamic SIMIPD Edit Protocol mode dynamic GPS info @ Wift parameters are negotiated by partners (dynamic) or already applied for 'static' mode GPS info @ Debug ICCP @ Enable more ICCP debug messages for 'Advanced Status' page Softflowd Tag name CyAP Statistics @ Custom key extension @ Tag name string, length must be 4, unified among ICCP partners Logout @ Used vian networks Vian007 vian123 VLAN tunnel @ Use a tunnel to transfer VLAN tags, otherwise one wift channel per VLAN network VLAN tunnel @ Use this MTU value for the tunnel device Min signal quality _e00 @ Mininal signal quality (BIND threshol) (dBm) @ Mininal signal quality (BIND threshol) (dBm)		
SIMPD Edit Protocol mode dynamic SIMPD Edit Protocol mode dynamic GPS Info @ Wifi parameters are negotiated by partners (dynamic) or already applied for 'static' mode GPSD Debug ICCP @ Enable more ICCP debug messages for 'Advanced Status' page Softford Tag name CyAP Statistics @ Tag name string, length must be 4, unified among ICCP partners Logout @ Custom key extension string: max.length 20, unified among ICCP partners Used vian networks vian007 vian123 VLAN tunnel @ Use a tunnel to transfer VLAN tags, otherwise one wifi channel per VLAN network VLAN tunnel @ Use this MTU value for the tunnel device Minimal signal quality _e0 @ Minimal signal quality (BIND threshold) (dBm)		
SNMP-Trap @ Vifi parameters are negotiated by partners (dynamic) or already applied for 'static' mode GPSD info @ Debug ICCP @ Enable more ICCP debug messages for 'Advanced Status' page Softlowd Tag name CyAP Network @ Tag name string, length must be 4, unified among ICCP partners Statistics Custom key extension [Logout @ Custom key extension @ Custom key extension string: max.length 20, unified among ICCP partners Used vlan networks Vian007 vlan123 @ Use this MTU value for the tunnel device VLAN tunnel @ Use this MTU value for the tunnel device @ Use this MTU value for the tunnel device Min signal quality _e0		
GPS Info @ Wift parameters are negotiated by partners (dynamic) or already applied for 'static' mode GPSD Debug ICCP @ Enable more ICCP debug messages for 'Advanced Status' page Softflowd Tag name CyAP Network @ Tag name string, length must be 4, unified among ICCP partners Custom key extension [Logout @ Custom key extension string: max.length 20, unified among ICCP partners Used vian networks Vian007 vian123 VLAN tunnel Isoo VLAN tunnel MTU 1500 @ Use this MTU value for the tunnel device Min signal quality		
GPSD Debug ICCP Image: CCP		
ICCP Image: CCP debug messages for 'Advanced Status' page SoftBowd Tag name CyAP Image: Custom key extension Image: Custom key extension string; length must be 4, unified among ICCP partners Logout Used vlan networks Vlan007 vlan123 VLAN tunnel Image: Custom key extension string; max.length 20, unified among ICCP partners VLAN tunnel Image: Custom key extension string; max.length 20, unified among ICCP partners VLAN tunnel Image: Custom key extension string; max.length 20, unified among ICCP partners VLAN tunnel Image: Custom key extension string; max.length 20, unified among ICCP partners VLAN tunnel Image: Custom key extension string; max.length 20, unified among ICCP partners VLAN tunnel Image: Custom key extension string; max.length 20, unified among ICCP partners VLAN tunnel Image: Custom key extension string; max.length 20, unified among ICCP partners VLAN tunnel Image: Custom key extension string; max.length 20, unified among ICCP partners Image: Custom key extension Image: Custom key extension string; max.length 20, unified among ICCP partners Image: Custom key extension Image: Custom key extension string; max.length 20, unified among ICCP partners Image: Custom key extension Image: Custom key extension string; max.length 20, unified among ICCP partners <td></td>		
Softflowd Tag name CyAP Network Image: Tag name string, length must be 4, unified among ICCP partners Statistics Custom key extension Image: Tag name string, length must be 4, unified among ICCP partners Logout Image: Custom key extension Image: Custom key extension string: max.length 20, unified among ICCP partners Logout Ved vlan networks vlan007 vlan123 VLAN tunnel Image: Custom key extension string: max.length 20, unified among ICCP partners VLAN tunnel Image: Custom key extension string: max.length 20, unified among ICCP partners VLAN tunnel Image: Custom key extension string: max.length 20, unified among ICCP partners VLAN tunnel Image: Custom key extension string: max.length 20, unified among ICCP partners VLAN tunnel Image: Custom key extension string: max.length 20, unified among ICCP partners VLAN tunnel Image: Custom key extension string: max.length 20, unified among ICCP partners VLAN tunnel Image: Custom key extension string: max.length 20, unified among ICCP partners Image: Custom key extension string: max.length 20, unified among ICCP partners Image: Custom key extension string: max.length 20, unified among ICCP partners Image: Custom key extension string: max.length 20, unified among ICCP partners Image: Custom key extension string: max.length 20, unified among ICCP		
Network Image: Constraint of the section of the se		
Statistics Image: Tag name string, length must be 4, unified among ICCP partners Logout Custom key extension Used vlan networks Image: VLAN tags, otherwise one wifi channel per VLAN network VLAN tunnel Image: String: max.length 20, unified among ICCP partners VLAN tunnel Image: String: max.length 20, unified among ICCP partners VLAN tunnel Image: String: max.length 20, unified among ICCP partners VLAN tunnel Image: String: max.length 20, unified among ICCP partners VLAN tunnel Image: String: max.length 20, unified among ICCP partners VLAN tunnel Image: String: max.length 20, unified among ICCP partners Image: String: max.length 20, unified among ICCP partners Image: String: max.length 20, unified among ICCP partners VLAN tunnel Image: String: max.length 20, unified among ICCP partners Image: String: max.length 20, unified among ICCP partners Image: String: max.length 20, unified among ICCP partners Image: String: max.length 20, unified among ICCP partners Image: String: max.length 20, unified among ICCP partners Image: String: max.length 20, unified among ICCP partners Image: String: max.length 20, unified among ICCP partners Image: String: max.length 20, unified among ICCP partners Image: String: String: max.length 20, unified among ICCP partners Image: String string: max.lengt		
Logout Used vlan networks VLAN tunnel VLAN		
Used vlan networks VLAN tunnel VLAN tunnel VLAN tunnel MTU 1500 WIse a tunnel device Min signal quality 60 Minimal signal quality (BIND threshold) [dBm]	1	
VLAN tunnel Image: Constraint of the tunnel of transfer VLAN tags, otherwise one wifi channel per VLAN network VLAN tunnel MTU 1500 Image: Constraint of the tunnel device Image: Constraint of the tunnel device Image: Constraint of the tunnel device Image: Constraint of the tunnel device Image: Constraint of the tunnel device Image: Constraint of the tunnel device Image: Constraint of the tunnel device Image: Constraint of the tunnel device	Custom key extension string: max.length 20, unified among ICCP partners	
Image: Constraint of the second se		
Image: Constraint of the second se		
Win signal quality -60 Minimal signal quality (BIND threshold) [dBm]		
Min signal quality -60 Minimal signal quality (BIND threshold) [dBm]		
Minimal signal quality (BIND threshold) [dBm]		
Quality check 0		
Orop ESTABLISHED if signal quality is lower than minimal for this time slot [sec] (0=disabled)		
Sustained discover 3		
Number of sustained discoveries as best partner in BIND/CONNECT phase		
Max Time 90		
Maximum CONNECT phase time [sec]		
Time extension 30		
CONNECT phase time extension [sec]		
Drop wait 300		
Wait [sec] before enter DROPPED state		
Drop retry 5		
Number of retries to switch from DROPPED to ESTABLISHED state		
ICCP parameters for radio1		
Enable protocol		
O Give ICCP exlusive usage on this radio		
Save & Apply		

Dynamic ICCP VLAN configuration

Note: Make sure that the VLAN tunnel checkbox is on.

Case 2: Static ICCP

Static ICCP can be used when you have no train carriage reconfigurations and the endpoints of VLAN tunnels are already known at time of configuration.

The configuration has to be performed on both ICCP partners.

a. Interfaces configuration

In addition to the steps described in Configurable Parameters, each VLAN (vlan007 and vlan123) must be configured as follows:

• Create new interface called 'vlan007' in the tab $\texttt{Network} \rightarrow \texttt{Interfaces}$

• When ask to specify a physical interface, create the custom interface eth0.007 then click on 'Save & Apply'

Further steps are also required regarding the configuration of the ICCP management interface:

- The WLAN modules from both ICCP partners have to be connected to each other. This means that on one radio the "Access Point (WDS)" mode must be selected and the mode "Client (WDS)" must be selected on the other radio. All other parameters such as SSID, encryption and operating frequency have also to be tuned to ensure the connection as for a standard Master/Client WLAN connection. All these setups can be configured in the tab Network → Wireless.
- Static IPs on the same subnet have to be set for the ICCP management interface in the tab '*Network*' \rightarrow 'Interfaces' (e.g. if the lan interface is selected as ICCP management interface including eth0 and wlan0, the IP address can be set to 10.0.0.1 on on "ICCP partner A" and to 10.0.0.2 on "ICCP partner B".)
- b. ICCP VLAN configuration

ICCP can be configured via the web interface as shown below, or via the command line with the commands:

On ICCP Partner A:

cfg_iccp -d -p static -r 0 -v vlan123 -v vlan007 -lip 172.16.0.1 -rip 172.16.0.2 -cidr 12

On ICCP Partner B:

cfg_iccp -d -p static -r 0 -v vlan123 -v vlan007 -lip 172.16.0.1 -rip 172.16.0.2 -cidr 12

Status	Inter Carriage Connection Protocol					
System	CCP provides automatic Wifi coupling between train carriages					
VPN	ICCP parameters for radio0					
Services						
Customize	Enable protocol					
SNMPD		Q Give ICCP exlusive usage on this radio				
SNMPD Edit	Protocol mode	static				
SNMP-Trap		🔿 1655 eccemptors are constituted by conteners (dynamic) as already, continuing for (static) mode				
GPS Info		Wifi parameters are negotiated by partners (dynamic) or already applied for 'static' mode				
GPSD	Debug ICCP					
ICCP		② Enable more ICCP debug messages for 'Advanced Status' page				
Softflowd	Used vlan networks	vlan007 vlan123				
Network	VLAN tunnel					
Statistics		We a tunnel to transfer VLAN tags, otherwise one wifi channel per VLAN network				
	VLAN tunnel MTU	1500				
Logout						
		Ise this MTU value for the tunnel device				
	Drop wait	300				
		Wait [sec] before enter DROPPED state				
	Local IP address	172.16.0.1/12				
		IP address for local WLAN tunnel side with netmask. If empty, IP is calculated from CyAP serial number.				
		For example: 172.16.0.1/12				
	Remote IP address	172.16.0.2/12				
		IP address for remote WLAN tunnel side with netmask. If empty, IP is calculated from CyAP serial number.				
		For example: 172.16.0.2/12				
	ICCP parameters for radio1					
	Enable protocol	0				
		Q Give ICCP exlusive usage on this radio				
	L	Save & Apply Save Reset				

Static ICCP VLAN configuration



СҮВОХ АР З

Note 2: The local and remote IP address fields have to be exchanged on the connection ICCP partner. The local IP is the one set on the ICCP management interface on the access point you are currently configuring. The screenshot above applies for ICCP partner A.

6.1.10 QoS

In the following example, a networking interface LAN or WLAN is prepared to use the Quality of Service function (QoS). The CyBox AP 3 implements a QoS function with scripts to configure traffic control ('tc' command), which reduces throughput at a selected interface. To see the effect, a performance test can be started with the built-in 'iperf' program to measure the throughput.

- Select Network $\rightarrow QoS$
- The default 'Interface' WAN is not activated and can be deleted.
 - In box Interfaces enter an existing interface name e.g. 'lan' an click button Add
 - Enter 1024 in the Download speed (kbit/s) field
 - Enter 1024 in the Upload speed (kbit/s) field
 - Activate checkbox Enable
 - Click Save & Apply

Do an 'iperf' performance test. The throughput should be about 10 Mbits/s. If a WLAN interface is bridged with the LAN port, the traffic control can even work on a single part of the bridge. To reduce the wireless traffic only, a new interface label must be added to <u>Network</u> → <u>Interfaces</u> menu e.g. WLAN. Then the new interface label has to be used in the QoS menu.

6.2 GPS

Some CyBox family members are equipped with an additional GNSS hardware module. The GPS antenna is routed to the front panel. Once an appropriate antenna is attached, the GPS signal is received and can be processed, if a version V3.03 or newer is installed. The GPS hardware supplies NMEA 0183 protocol on the second serial port, which is converted into a human-readable form.

6.2.1 GPS activation

The GPS is disabled by default. It can be enabled via the web interface. Enter $System \rightarrow GPS$ Info and check Enable.

Status	GPS Information			
System VPN	Read GPS information from internal GPS chip and Modem devices.			
Services	- Interfaces			
Customize	Enable	0		
SNMPD SNMPD Edit	Raw output	Enable raw output from GPS source		
SNMP-Trap GPS Info	Interface name	gps		
GPSD	······	Operation of the GPS Interface name		
ICCP Softflowd Network	Device name	ttyS1 Specifies the serial output device of GPS source		
Statistics	Speed unit	km/h 💌		

GPS Activation

6.2.2 GPS status

The GPS information will show on the Status \rightarrow Advanced of the web interface. The next figure shows an example available immediately after startup. And the figure below provides the same status after the receiver has calibrated itself. The table below provides an interpretation of the GPS status data.

Status	Module Information Revision Information Temperature Sensors GPS Sensors ICCP Self Test License
Overview	GPS Information
Advanced	
Firewall	Internal GPS
Routes	Status: V Quality: 0
System Log	Sat: 0
Kernel Log	Sun Jan 4 00:17:03 2009 N: 0.000000
Processes	E: 0.000000 N: 0°0'0.000"
Realtime Graphs	E: 0°0'0.000"
Load Balancing	Alt: 82.00m Speed: 0 km/h
System	
VPN	
Services	
Network	
Statistics	
Logout	

GPS Info immediately after startup

Status	Module Information Revision Information Temperature Sensors GPS Sensors
Overview	GPS Information
Advanced	
Firewall	Internal GPS
Routes	Status: A Quality: 1
System Log	Sat: 13
Kernel Log	Thu Sep 10 12:38:31 2020 N: 49.960240
Processes	E: 8.258405 N: 49°57'36.864"
Realtime Graphs	E: 8°15'30.258" Alt: 147.57m
Load Balancing	Speed: 0 km/h
System	

Reliable GPS Info after Hardware Calibration

GPS Status Data:

	Data Item	Value	Description
--	-----------	-------	-------------

Integrity	А	Active
	V	Void
Quality	0	Invalid
	1	GPS fix (SPS)
	2	DGPS fix
	3	PPS fix
	4	Real Time Kinematic
	5	Float RTK
	6	Estimated
	7	Manual input mode
	8	Simulation mode

6.2.3 SNMP for GPS

See chapter SNMP Support for GPS

6.3 System

6.3.1 Configuration Backups

Configuration is managed in the tab System → Backup/Flash Firmware.

Status	Flash operations					
System						
System	Actions Configuration					
Administration	Backup					
Startup	Click "Generate archive" to download a tar archive of the current configuration files.					
Scheduled Tasks	Download backup Generate archive					
Mount Points	Restore					
Backup / Flash Firmware	To restore configuration files, you can upload a previously generated backup archive here. To reset the firmware to its initial state, click "Perform reset" (only possible with squashfs images).					
Custom Commands						
License		Perform reset				
Reboot	Restore backup	Durchsuchen Keine Datei ausgewählt. Upload archive				
VPN		Oustom files (certificates, scripts) may remain on the system. To prevent this, perform a factory-reset first.				
Services						
Network	Save mtdblock contents					
Statistics	Click "Save mtdblock" to download specified mtdblock file. (NOTE: THIS FEATURE IS FOR PROFESSIONALS!)					
	Choose mtdblock	u-boot 🔹				
Logout	Download mtdblock	Save mtdblock				
	Flash new firmware image					
	- Upload a sysupgrade-compatible image here to replace the running firmware. Check "Keep settings" to retain the current configuration (requires a compatible firmware image).					
	Keep settings					
	Image	Durchsuchen Keine Datei ausgewählt. Flash image				

Configuration Backup Settings

a. Restore factory settings

Perform reset restores factory settings and performs a reboot.

b. Export configuration

Use the Generate archive button to export a configuration backup.

The generated configuration tar archive is not hardware-specific and may be distributed to other access points, as long as they share the same model and the same firmware version.

Note: Configuration archives are not compatible between firmware revisions 4.x and 17.xx.yy.

With the Upload archive... button you can restore a previously saved configuration. After restoring a configuration, the access point will reboot.

c. Import configuration

Before restoring a configuration archive, make sure that the factory settings have been restored in order to avoid any conflict between your old and new configuration. The configuration file must be named according to the pattern backup-*.tar.gz and can then be uploaded in the Restore backup field.

6.3.2 Firmware Upgrade

The procedure to update the device firmware with a new image is shown below.

2	11	IC	÷.	0	M	C
	u	10	L.	С	ш	0
	-					

	Flash operations		
Mation Configuration			
Backup			
Click "Generate archive" to download a tar archive of the current configuration files.			
lownload backup	Generate archive		
rtoro			
To restore configuration files, you can upload a previously generated backup archive here. To reset the firmware to its initial state, click "Perform reset" (only possible with squashfs images).			
leset to defaults	Perform reset		
lestore backup	Durchsuchen Keine Datei ausgewählt. Upload archive		
	Custom files (certificates, scripts) may remain on the system. To prevent this, perform a factory-reset first.		
Cusioni nies (cerunicates, scripts) may remain on the system. To prevent unis, perioritra factory-reset trist.			
Save mtdblock contents			
Click "Save mtdblock" to download specified mtdblock file. (NOTE: THIS FEATURE IS FOR PROFESSIONALS!)			
hoose mtdblock	u-boot _		
lownload mtdblock	Save mtdblock		
Flash new firmware image			
Upload a sysupgrade-compatible image here to replace the running firmware. Check "Keep settings" to retain the current configuration (requires a compatible firmware image).			
eep settings	0		
nage	Durchsuchen V20.14_cyap2-lzma.itb Flash image		
	k "Generate archive" to download a tar archive of the current configuration files pwnload backup store astore configuration files, you can upload a previously generated backup archiv asset to defaults astore backup re mtdblock contents k "Save mtdblock" to download specified mtdblock file. (NOTE: THIS FEATURE toose mtdblock wnload mtdblock sh new firmware image bad a sysupgrade-compatible image here to replace the running firmware. Check tep settings		

Firmware Update Settings

Firmware Updates are provided as binary images with the extension .itb and will be uploaded from the host computer. Keep settings should always be **cleared** to ensure not to mixup old and new config switches. The uploaded image has a MD5 checksum that must be confirmed in the following dialog.

WARNING: Do NOT POWER OFF the access point while upgrading/restoring firmware to flash. Remember that if ``Keep settings`` checkbox is cleared, the device will revert to its network default address after restart.

6.3.3 Reboot

The device can be rebooted on the System \rightarrow Reboot tab.

6.3.4 Reset Button

The operations which can be done with the reset button are: reboot, triggering the emergency mode, restoring factory settings.

a. Restore factory settings

After booting, a factory reset can be triggered by pressing the reset button with a pin for more than 5 seconds. The Fail LED will blink in green and after a few seconds the device will reboot with the default configuration.

A reboot can be triggered by pressing the reset button with a pin for less than 2 seconds.

6.3.5 Emergency Mode

Emergency mode should only be needed in case of system firmware upgrade or crash restore.

The CyBox AP family uses at least five partitions in flash memory. The first flash device contains the low level firmware U-Boot. The second flash device holds an emergency image of OpenWrt/Linux and the third device contains the standard image of OpenWrt/Linux. The fourth flash device contains a journaling flash file system partition with user configuration settings and a customer partition. Normally the standard OpenWrt/Linux image is loaded with U-Boot and checked with MD5 sum against errors. If checksums are valid the linux boots and access point service starts. User configuration parameters are loaded and applied from the JFFS partition.

In case of a damaged standard image (OpenWrt/Linux in third flash) U-Boot detects a MD5 checksum error and tries to start the emergency system image from second flash. While booting no user configuration settings are applied. The CyBox AP 3 comes up with network default address 192.168.100.1 (user=root, password=root) and Wifi disabled. The Fail LED blinks orange (red and green on) and the web interface background is orange, as Figure indicates. All configuration settings are volatile. This system should only be used to Upgrade/Restore a working firmware image to second flash via *Backup / Flash Firmware* menu.

ELTEC

systems

Status	Flash operations		
System	Actions		
System			
Administration	Backup		
Startup	Click "Generate archive" to download a tar archive of the current configuration files.		
Scheduled Tasks	Download backup	Generate archive	
Mount Points	Restore		
Backup / Flash Firmware			
Custom Commands	To restore configuration files, you can upload a previously generated backup archive here. To reset the firmware to its initial state, click "Perform reset" (only possible with squashfs images).		
License	Reset to defaults	Perform reset	
Reboot	Restore backup		
VPN		Durchsuchen Keine Datei ausgewählt. Upload archive	
Services		② Custom files (certificates, scripts) may remain on the system. To prevent this, perform a factory-reset first.	
Network			
Statistics	Save mtdblock contents		
	Click "Save mtdblock" to download specified mtdblock file. (NOTE: T	HIS FEATURE IS FOR PROFESSIONALS!)	
Logout	Choose mtdblock	u-boot _	
	Download mtdblock	Save mtdblock	
	Flash new firmware image		
	Upload a sysupgrade-compatible image here to replace the running f image).	irmware. Check "Keep settings" to retain the current configuration (requires a compatible firmware	
	Keep settings		
	Image	Durchsuchen Keine Datei ausgewählt. Flash image	
owered by LuCI (V20.14)			

Emergency System Indication

Emergency mode can also be entered by holding the reset button pressed for 5 seconds at the beginning of the boot phase.

Note: Normally, the blue background indicates the standard mode and the orange background indicates emergency mode. But many web browsers keep the colours in cache, which means that the wrong colour can be displayed. To ensure that the correct one is shown, open a new window in private or incognito mode before consulting the web interface.

7 SNMP

7.1 SNMP Protocol Support

Firmware implementations before 2020 only have protocol support for version **v1** and **v2c**. Since 2020 the SNMP protocol **v3** is also included in every CyBox firmware. The **v1**, **v2c** protocol variants are present with factory default setup. In factory default setup only read access is permitted.

Status	SNMPD				
System VPN	SNMPD is a master daemon/agent for SNMP, from the net-snmp project. This LuCI applet covers basic configuration options. See documentation for manual configuration.				
Services	Protocol activation				
Customize	Enable v1 protocol				
SNMPD	Enable v2c protocol				
SNMPD Edit SNMP-Trap	Enable v3 protocol				
GPS Info	Agent settings				
GPSD ICCP	The address the agent should listen on	UDP:161			
Softflowd		Eg: UDP:161, or UDP:10.5.4.3:161 to only listen on a given interface			
Network Statistics	AgentX settings	5			
	The address the agent should allow agentX connections to	/var/run/agentx.sock			
Logout		This is only necessary if you have subagents using the agentX socket protocol. Note that agentX requires TCP transport			
	Protocol V3 settings				
	Create Protocol V3 User This section contains no values yet Add com2sec security				
	PUBLIC				
	secname	ro			
	source	default			
	community	public			
	PRIVATE				

SNMPD factory default settings with protocol v1 and v2c enabled

7.2 SNMP V3 Protocol Support

Before any **v3** protocol access can be executed one or more V3 User Accounts have to be created. To add a new **v3** User Account, the name must be entered case sensitve. Later the WUI is showing the User Account name in upper case.

Protocol V3 settings
Create Protocol V3 User
This section contains no values yet
SHAAESUser Add

Add new v3 User Account

The new User Account can be created as read-only, or with read-write permission. The authentication protocol is either **MD5** or **SHA** (preferred). If a authentication protocol is selected the authentication passphrase must also be given. For data paket encryption select **DES** or **AES** (preferred) and also apply a passphrase. For demonstration use the same settings as in figure below to copy and paste them in examples.

Protocol V3 settings		
Create Protocol V3 User		
		Delete
SHAAESUSER		
User Name	SHAAESUser	
User Access	Read-Write User •	
Authentication Protocol	SHA	
Authentication Passphrase	sha_password	
Privacy Protocol	AES	
Privacy Passphrase	aes_passphrase	
Privacy Passphrase	aes_passphrase	

Demo user account settings

The default protocols v1 and v2c should be disabled, when using SNMP-V3 protocol.

Services	Protocol activation	
Customize	Enable v1 protocol	
SNMPD SNMPD Edit	Enable v2c protocol	
SNMP-Trap	Enable v3 protocol	

Activate only SNMP-V3 protocol

After all new settings are entered press the Save & Apply. Then the SNMPD service will restarted automatically.

7.2.1 SNMP V3 Protocol Examples

Read access with **snmpget**: Get order identifier

The command:

Returns:

iso.3.6.1.4.1.2021.8.1.2.100.101.1 = STRING: "CYAPW-1057PO"

Read access with **snmpwalk**: Get firmware version

The command:

Returns:

```
iso.3.6.1.4.1.2021.8.1.2.103.1.1 = INTEGER: 1
iso.3.6.1.4.1.2021.8.1.2.103.2.1 = STRING: "firmware_version"
iso.3.6.1.4.1.2021.8.1.2.103.3.1 = STRING: "/usr/bin/eltec_version"
```

ELTEC

```
iso.3.6.1.4.1.2021.8.1.2.103.100.1 = INTEGER: 0
iso.3.6.1.4.1.2021.8.1.2.103.101.1 = STRING: "20.14"
iso.3.6.1.4.1.2021.8.1.2.103.102.1 = INTEGER: 0
iso.3.6.1.4.1.2021.8.1.2.103.103.1 = ""
```

Write access with snmpset: Set a new system hostname and reload system settings

Use the following sequence to set the new hostname:

The new system hostname can be checked on web Status page.

7.3 SNMP Basic Functions

The SNMP service is included in CyBox AP 3 Starting with firmware Version 2.6. The service is enabled, if a valid configuration file '/etc/config/snmpd' is present and service startup is not disabled. On system start this configuration file is parsed and translated into a 'snmpd.conf' file which is required by the SNMP daemon. The 'snmpd.conf' is stored in '/var/run' and a symbolic link is available under '/etc/snmp'.

There is a basic web interface provided for SNMP private / public configuration under Services \rightarrow SNMPD. The whole configuration file is quite large (~120KB) and can be modified on command line with UCI commands or by editing the configuration file with Services \rightarrow SNMPD-Edit edit window. The current implementation is automatically generated from a build script.

The OpenWrt default configuration provides a set of standard MIB files with OID .1.3.6.1.2.1 (iso.org.dod.internet.mgmt.mib-2). ELTEC also provides an extension for the default configuration, using the UC DAVIS (University of California, Davis) MIB object (UCD-SNMP-MIB MIB document as .1.3.6.1.4.1.2021) to map many configuration settings with a wrapper shell for reading '/usr/sbin/get_snmp' and one for writing '/usr/sbin/get_snmp' single entries in the configuration files located under '/etc/config'. The 'get_snmp' script provides also information about WLAN to SSID assignment, WLAN bitrates, signal quality, etc. Most of this information is gained via UCI commands for reading and writing system configuration settings.

/etc/snmp/snmpd.conf # Symlink to SNMPD config file (automatically created)

/etc/config/snmpd # OpenWrt configuration file

See Appendix 10 for a SNMP command OID overview.

7.4 SNMP Read and Write Authorizations

The CyBox AP 3 runs a local SNMP daemon, which currently is configured for two access groups:

- By default, group "public" allows unrestricted read-only access
- Group "private" allows a single specified host to read and write. By default, "localhost" is specified i.e. only the local administrative user on CyBox AP 3 is allowed for SNMP write operations.

This address can be changed by means of an UCI command. Assuming to be logged-in on a CyBox AP 3 via SSH as administrative user, the following command would allow re-specifying the IP address of the "private" group:

```
root@CyBoxAP:~# uci set snmpd.private.source=<ccu>
root@CyBoxAP:~# uci commit snmpd
root@CyBoxAP:~# /etc/init.d/snmpd restart
```

Where *<ccu>* refers to the IP address (or hostname) of the remote host which is allowed to perform SNMP write operations. The keyword "default" instead of a specific address allows any hosts to access the SNMP demon.

Similarly, the address of the "public" group can be changed:

```
root@CyBoxAP:~# uci set snmpd.public.source=<ccu>
root@CyBoxAP:~# uci commit snmpd
root@CyBoxAP:~# /etc/init.d/snmpd restart
```

Note: Generally local UCI commands on the CyBox AP 3 should be used for handling the configuration of the SNMP demon. Run '*uci show snmpd*' to view the current settings.

Alternatively, the public and private sources can be modified with the web interface in the field '*com2sec security*' of the tab '*Services*' \rightarrow '*SNMPD*'.

PUBLIC		
secname	го	
source	default	
community	public	
PRIVATE		
secname	rw	
source	localhost	

SNMPD change 'com2sec security' for write access

7.5 SNMP Commands

The CyBox AP 3 SNMP demon supports the following commands:

- snmpget
- snmpset
- snmpstatus
- snmptest
- snmptrap
- snmpwalk

A special case arises when snmpset writes to non-MIB extensions. In this case, there is an asymmetry between snmpget and snmpset with respect to OIDs. Reading (snmpget) requires the complete numeric identifier including the server-specific extension. Writing (snmpset) accepts only the "extEntry" trunk "iso.3.6.1.4.1.2021.8.1", while the server-specific name of the object must be passed as first argument.

The assignment of names and OID numbers can be found by executing snmpwalk.

7.6 SNMP Read (snmpwalk and snmpget)

The following chapters describe the read and write access via console commands.

7.6.1 Reading System Information

```
boardname 1.3.6.1.4.1.2021.8.1.2.100
serial_number 1.3.6.1.4.1.2021.8.1.2.101
uboot_version 1.3.6.1.4.1.2021.8.1.2.102
firmware_version 1.3.6.1.4.1.2021.8.1.2.103
config_version 1.3.6.1.4.1.2021.8.1.2.104
uptime 1.3.6.1.4.1.2021.8.1.2.105
loadavg 1.3.6.1.4.1.2021.8.1.2.106
temperature 1.3.6.1.4.1.2021.8.1.2.106
usi_get 1.3.6.1.4.1.2021.8.1.2.108
customl 1.3.6.1.4.1.2021.8.1.2.109
custom2 1.3.6.1.4.1.2021.8.1.2.100
custom3 1.3.6.1.4.1.2021.8.1.2.110
mpstat 1.3.6.1.4.1.2021.8.1.2.112
```

The command

snmpwalk -c public -v 2c 192.168.100.1 1.3.6.1.4.1.2021.8.1.2.100

will deliver

```
iso.3.6.1.4.1.2021.8.1.2.100.1.1 = INTEGER: 1
iso.3.6.1.4.1.2021.8.1.2.100.2.1 = STRING: "boardname"
iso.3.6.1.4.1.2021.8.1.2.100.3.1 = STRING: "/bin/cat /tmp/sysinfo/eeprom/BOARDNAME"
iso.3.6.1.4.1.2021.8.1.2.100.100.1 = INTEGER: 0
iso.3.6.1.4.1.2021.8.1.2.100.101.1 = STRING: "CYAP.-V-W8IRQWWEUPX"
iso.3.6.1.4.1.2021.8.1.2.100.102.1 = INTEGER: 0
iso.3.6.1.4.1.2021.8.1.2.100.103.1 = ""
```

MIB name:

iso.3.6.1.4.1.2021.8.1.2.100.2.1 = STRING: "boardname"

Function executed on CyBox AP 3:

iso.3.6.1.4.1.2021.8.1.2.100.3.1 = STRING: "/bin/cat /var/BOARDNAME"

Error code from function call:

iso.3.6.1.4.1.2021.8.1.2.100.100.1 = INTEGER: 0

Return value from function call:

iso.3.6.1.4.1.2021.8.1.2.100.101.1 = STRING: "CYAP.-V-W8IRQWWEUPX"

7.6.2 Reading SNMP Object Information

The main problem to access a network device (WLAN or LAN) is that the listing order depends on the creation order made by user when the config file is being edited. The fact that network/interface naming is free to choose and that UCD MIB object names are static, makes it necessary to use predefined names like:

```
• network0, network1 ... network9
```

• wireless0, wireless1 ... wireless19

Note: A normal CyBox AP 3 configuration consists of six wireless interfaces, but there are up to twenty interfaces possible, so snmpwalk will result in up to 80 percent of undefined (Empty UCI entry) values.

The following objects are available to determine the actual network/wireless ordering.

7.6.2.1 Readout current Network Device Order

The command

snmpwalk -c public -v 2c 192.168.100.1 1.3.6.1.4.1.2021.8.1.2.150

delivers

```
iso.3.6.1.4.1.2021.8.1.2.150.1.1 = INTEGER: 1
iso.3.6.1.4.1.2021.8.1.2.150.2.1 = STRING: "network_order"
iso.3.6.1.4.1.2021.8.1.2.150.3.1 = STRING: "/etc/snmp/get_cyboxap network_order"
iso.3.6.1.4.1.2021.8.1.2.150.100.1 = INTEGER: 0
iso.3.6.1.4.1.2021.8.1.2.150.101.1 = STRING: "loopback=lo" **<--- network0**
iso.3.6.1.4.1.2021.8.1.2.150.101.2 = STRING: "lan=eth0" **<--- network1**
iso.3.6.1.4.1.2021.8.1.2.150.101.3 = STRING: "vlan007=eth0.7" **<--- network2**
iso.3.6.1.4.1.2021.8.1.2.150.101.4 = STRING: "vlan007=eth0.123" **<--- network3**
iso.3.6.1.4.1.2021.8.1.2.150.101.5 = STRING: "vlan500=eth0.500" **<--- network4**
iso.3.6.1.4.1.2021.8.1.2.150.101.6 = STRING: "cfg_net=eth0.999" **<--- network5**
iso.3.6.1.4.1.2021.8.1.2.150.103.1 = ""</pre>
```

Example:

IP address of LAN interface 'cfg_net' will be (network5 starts at 550):

network5.ipaddr 1.3.6.1.4.1.2021.8.1.2.552

The command

snmpget -c public -v 2c 192.168.100.1 1.3.6.1.4.1.2021.8.1.2.552.101.1

delivers

iso.3.6.1.4.1.2021.8.1.2.552.101.1 = STRING: "192.168.99.98"

7.6.2.2 Readout SSID / WIFI Interface Order

The following command shows the order of the Wifi interfaces.

```
snmpwalk -c public -v 2c 192.168.100.1 1.3.6.1.4.1.2021.8.1.2.151
iso.3.6.1.4.1.2021.8.1.2.151.1.1 = INTEGER: 1
iso.3.6.1.4.1.2021.8.1.2.151.2.1 = STRING: "ssid_order"
iso.3.6.1.4.1.2021.8.1.2.151.3.1 = STRING: "/etc/snmp/get_cyboxap ssid_order"
iso.3.6.1.4.1.2021.8.1.2.151.100.1 = INTEGER: 0
iso.3.6.1.4.1.2021.8.1.2.151.101.1 = STRING: "CyAP0_00486889_00486886_EST0" **<--- wireless0**
iso.3.6.1.4.1.2021.8.1.2.151.101.2 = STRING: "Guest_007" **<--- wireless1**
iso.3.6.1.4.1.2021.8.1.2.151.101.3 = STRING: "CyAP0_00486889_00486886_vlan007" **<--- wireless2**
iso.3.6.1.4.1.2021.8.1.2.151.101.4 = STRING: "CyAP0_00486889_00486886_vlan007" **<--- wireless3**
iso.3.6.1.4.1.2021.8.1.2.151.101.5 = STRING: "CyAP0_00486889_00486886_vlan123**" <--- wireless3**
iso.3.6.1.4.1.2021.8.1.2.151.101.6 = STRING: "CyAP0_00486889_00486886_vlan500" **<--- wireless4**
iso.3.6.1.4.1.2021.8.1.2.151.101.6 = STRING: "CyAP0_00486889_00486886_vlan500" **<--- wireless5**
iso.3.6.1.4.1.2021.8.1.2.151.101.7 = STRING: "CyAP0_00486889_00486886_vlan500" **<--- wireless5**
iso.3.6.1.4.1.2021.8.1.2.151.101.6 = STRING: "CyAP0_00486889_00486886_vlan500" **<--- wireless5**
iso.3.6.1.4.1.2021.8.1.2.151.101.8 = STRING: "VIP_500" **<--- wireless7**</pre>
```

iso.3.6.1.4.1.2021.8.1.2.151.102.1 = INTEGER: 0
iso.3.6.1.4.1.2021.8.1.2.151.103.1 = ""

7.6.2.3 Readout Network Device to SSID Assignment

The following command shows the order of the Wifi interfaces.

```
snmpwalk -c public -v 2c 192.168.100.1 1.3.6.1.4.1.2021.8.1.2.152
iso.3.6.1.4.1.2021.8.1.2.152.1.1 = INTEGER: 1
iso.3.6.1.4.1.2021.8.1.2.152.2.1 = STRING: "wlan_ssid"
iso.3.6.1.4.1.2021.8.1.2.152.3.1 = STRING: "/etc/snmp/get_cyboxap wlan_ssid"
iso.3.6.1.4.1.2021.8.1.2.152.100.1 = INTEGER: 0
iso.3.6.1.4.1.2021.8.1.2.152.101.1 = STRING: "wlan0 : \\"CyAP0_00486889_00486886_EST0\\""
iso.3.6.1.4.1.2021.8.1.2.152.101.2 = STRING: "wlan0 : \\"CyAP0_00486889_00486886_EST0\\""
iso.3.6.1.4.1.2021.8.1.2.152.101.3 = STRING: "wlan0-1 : \\"CyAP0_00486889_00486886_vlan007\\""
iso.3.6.1.4.1.2021.8.1.2.152.101.3 = STRING: "wlan0-2 : \\"CyAP0_00486889_00486886_vlan123\\""
iso.3.6.1.4.1.2021.8.1.2.152.101.4 = STRING: "wlan0-3 : \\"CyAP0_00486889_00486886_vlan500\\""
iso.3.6.1.4.1.2021.8.1.2.152.101.5 = STRING: "wlan0-4 : \\"CyAP0_00486889_00486886_cfg_net\\""
iso.3.6.1.4.1.2021.8.1.2.152.101.6 = STRING: "wlan0-1 : \\"Guest_07\\""
iso.3.6.1.4.1.2021.8.1.2.152.101.6 = STRING: "wlan1-1 : \\"Guest_123\\""
iso.3.6.1.4.1.2021.8.1.2.152.101.7 = STRING: "wlan1-2 : \\"VIP_500\\""
iso.3.6.1.4.1.2021.8.1.2.152.101.8 = STRING: "wlan1-2 : \\"VIP_500\\""
```

Note 1: This assignment may change every time a specific SSID is disabled or enabled and the wireless interface is restarted. The corresponding Linux WLAN device for a SSID is needed to readout current assoclist, bitrates and signal quality values.

Note 2: The order/assignment functions 150, 151 and 152 should not be polled in an application, since they require some CPU resources. The network status should only be readout once after system start and every time operator causes a change in the network layout.

Example:

Readout assoclist, bitrate and signal quality from wlan0-2 (CyAP0_00486889_00486886_vlan123)

```
assoclist_wlan0-2 1.3.6.1.4.1.2021.8.1.2.202
bitrate_wlan0-2 1.3.6.1.4.1.2021.8.1.2.242
signal_wlan0-2 1.3.6.1.4.1.2021.8.1.2.282
```

The command

snmpget -c public -v 2c 192.168.100.1 1.3.6.1.4.1.2021.8.1.2.202.101.1

returns the assoclist

iso.3.6.1.4.1.2021.8.1.2.202.101.1 = STRING: "06:0E:8E:67:08:64"

The command

snmpget -c public -v 2c 192.168.100.1 1.3.6.1.4.1.2021.8.1.2.242.101.1

returns the bitrate information

iso.3.6.1.4.1.2021.8.1.2.242.101.1 = STRING: "65.0 Mbit/s"

The command

snmpget -c public -v 2c 192.168.100.1 1.3.6.1.4.1.2021.8.1.2.282.101.1

returns the signal quality information

iso.3.6.1.4.1.2021.8.1.2.282.101.1 = STRING: "Link Quality: 70/70 Signal: -33 dBm Noise: -95 dBm "

7.7 SNMP Write (snmpset)

By default all SNMP write control is restricted to localhost. Refer to chapter 8.1 to enable write access.

A write command to the CyBox AP 3 is always done on the same UCD MIB OID '1.3.6.1.4.1.2021.8.1'. The write operation requires a string parameter, which is parsed with '/etc/snmp/set_cyboxap' and translated into a system internal call on the CyBox AP 3. Consider that all writes to a configuration item are permanently stored in the overlay file system and will be present after next power cycle.

Usage of the SNMPSET system call:

snmpset -c private -v 2c <IPv4> 1.3.6.1.4.1.2021.8.1 s <command string or set entry string>

The given parameter string can be for example:

Command Type	Parameter String
Direct command	<pre>"radio0_up" "radio0_down" "modem0_up" "modem0_down" see Appendix for all commands "reboot"</pre>
System service action	"service <name> <action>"</action></name>
UCI configuration call	"uci <command/> <config>.<section> [<option>]=<value>"</value></option></section></config>
Configuration set to new value	"network <index>.<entry> <value>" "radio<index>.<entry> <value>" "wireless<index>.<entry> <value>"</value></entry></index></value></entry></index></value></entry></index>

7.7.1 Direct command

7.7.1.1 Reboot

snmpset -c private -v 2c 192.168.100.1 1.3.6.1.4.1.2021.8.1 s "reboot"

7.7.2 Edit configuration using Object Identifier (OID)

7.7.2.1 Set a new IP address

snmpset -c private -v 2c 192.168.100.1 1.3.6.1.4.1.2021.8.1 s "network5.ipaddr 192.168.20.20"
snmpset -c private -v 2c 192.168.100.1 1.3.6.1.4.1.2021.8.1 s "uci commit network"
snmpset -c private -v 2c 192.168.100.1 1.3.6.1.4.1.2021.8.1 s "service network reload"

7.7.2.2 Set a new SSID

snmpwalk -c public -v 2c 192.168.100.1 1.3.6.1.4.1.2021.8.1.2.151
iso.3.6.1.4.1.2021.8.1.2.151.1.1 = INTEGER: 1
iso.3.6.1.4.1.2021.8.1.2.151.2.1 = STRING: "ssid_order"
iso.3.6.1.4.1.2021.8.1.2.151.3.1 = STRING: "/etc/snmp/get_cyboxap ssid_order"
iso.3.6.1.4.1.2021.8.1.2.151.100.1 = INTEGER: 0
iso.3.6.1.4.1.2021.8.1.2.151.101.1 = STRING: "CyAP0_00486889_00486886_EST0"
iso.3.6.1.4.1.2021.8.1.2.151.101.2 = STRING: "Guest_007"
iso.3.6.1.4.1.2021.8.1.2.151.101.4 = STRING: "CyAP0_00486889_00486886_vlan007"
iso.3.6.1.4.1.2021.8.1.2.151.101.4 = STRING: "CyAP0_00486889_00486886_vlan007"
iso.3.6.1.4.1.2021.8.1.2.151.101.5 = STRING: "CyAP0_00486889_00486886_vlan007"
iso.3.6.1.4.1.2021.8.1.2.151.101.6 = STRING: "CyAP0_00486889_00486886_vlan123"
iso.3.6.1.4.1.2021.8.1.2.151.101.6 = STRING: "CyAP0_00486889_00486886_cfg_net"
iso.3.6.1.4.1.2021.8.1.2.151.101.7 = STRING: "Guest_123" <= change index 6
iso.3.6.1.4.1.2021.8.1.2.151.102.1 = INTEGER: 0
iso.3.6.1.4.1.2021.8.1.2.151.101.8 = STRING: "UP_500"
iso.3.6.1.4.1.2021.8.1.2.151.102.1 = INTEGER: 0
iso.3.6.1.4.1.2021.8.1.2.151.103.1 = ""</pre>

Get radio module from wireless6.device=1.3.6.1.4.1.2021.8.1.2.1440 (may be omitted if SSID-radio is known):

snmpget -c public -v 2c 192.168.100.1 1.3.6.1.4.1.2021.8.1.2.1440.101.1

delivers

```
iso.3.6.1.4.1.2021.8.1.2.1440.101.1 = STRING: "radiol"
snmpset -c private -v 2c 192.168.100.1 1.3.6.1.4.1.2021.8.1 s "wireless6.ssid New_345"
snmpset -c private -v 2c 192.168.100.1 1.3.6.1.4.1.2021.8.1 s "uci commit wireless"
snmpset -c private -v 2c 192.168.100.1 1.3.6.1.4.1.2021.8.1 s "service network reload"
```

7.7.2.3 Set a new Macfilter

Apply a new 'macfilter' on the access point "VIP_500". Specific user mac is excluded.

```
snmpset -c private -v 2c 192.168.100.1 1.3.6.1.4.1.2021.8.1 s
"wireless7.macfilter deny"
```

Single user:

```
snmpset -c private -v 2c 192.168.100.1 1.3.6.1.4.1.2021.8.1 s
"wireless7.maclist 11:22:33:44:55:66"
```

Multiple user:

```
snmpset -c private -v 2c 192.168.100.1 1.3.6.1.4.1.2021.8.1 s "uci
add_list wireless.@wifi-\ face[7].maclist=11:22:33:44:55:66"
snmpset -c private -v 2c 192.168.100.1 1.3.6.1.4.1.2021.8.1 s "uci
add_list wireless.@wifi-face[7].maclist=22:33:44:55:66:77"
snmpset -c private -v 2c 192.168.100.1 1.3.6.1.4.1.2021.8.1 s "uci
commit wireless"
snmpset -c private -v 2c 192.168.100.1 1.3.6.1.4.1.2021.8.1 s "service
network reload"
```

7.7.3 Edit configuration parameters, create new fields and delete items

If a 'config.section.option' is known, the 'uci set' command call can be used to read and modify any existing configuration item. If a snmpset command with a string "uci <command> config-item=new-value" is executed, it marks the config-item. The next snmpget call with '1.3.6.1.4.1.2021.8.1.2.108' (uci_get) remembers the last config-item and returns the curre nt value (read-back function). If the snmpset was executed without the string

part "=new-value" only the config-item marker is set. This can be used to readout an item (no OID) without modifying it.

Note: Remember to commit changes in order to save then with the command 'uci commit'.

7.7.3.1 Set new Hostname

Hostname is configured in '/etc/config/system' (no OID).

The commands

snmpset -c private -v 2c 192.168.100.1 1.3.6.1.4.1.2021.8.1 s "uci set system.@system[0].hostname"

snmpwalk -c public -v 2c 192.168.100.1 1.3.6.1.4.1.2021.8.1.2.108

will deliver

```
iso.3.6.1.4.1.2021.8.1.2.108.1.1 = INTEGER: 1
iso.3.6.1.4.1.2021.8.1.2.108.2.1 = STRING: "uci_get"
iso.3.6.1.4.1.2021.8.1.2.108.3.1 = STRING: "/usr/sbin/get_snmp
uci_get"
iso.3.6.1.4.1.2021.8.1.2.108.100.1 = INTEGER: 0
iso.3.6.1.4.1.2021.8.1.2.108.101.1 = STRING:
"system.@system[0].hostname=CyBoxAP"
iso.3.6.1.4.1.2021.8.1.2.108.102.1 = INTEGER: 0
iso.3.6.1.4.1.2021.8.1.2.108.103.1 = ""
```

Use the following sequence to set the new hostname

```
snmpset -c private -v 2c 192.168.100.1 1.3.6.1.4.1.2021.8.1 s "uci set
system.@system[0].hostname=CYAP-14"
snmpset -c private -v 2c 192.168.100.1 1.3.6.1.4.1.2021.8.1 s "uci
commit system"
snmpset -c private -v 2c 192.168.100.1 1.3.6.1.4.1.2021.8.1 s "service
system reload"
```

7.7.3.2 Creating a system configuration description text

The regular firmware configuration does not provide such information. The following command sequence

```
snmpset -c private -v 2c 192.168.100.1 1.3.6.1.4.1.2021.8.1 s "uci set
system.@system[0].config_description=Version 1.1 Beta ABC"
snmpwalk -c public -v 2c 192.168.100.1 1.3.6.1.4.1.2021.8.1.2.108
```

delivers

```
iso.3.6.1.4.1.2021.8.1.2.108.1.1 = INTEGER: 1
iso.3.6.1.4.1.2021.8.1.2.108.2.1 = STRING: "uci_get"
iso.3.6.1.4.1.2021.8.1.2.108.3.1 = STRING: "/usr/sbin/get_snmp
uci_get"
```

```
iso.3.6.1.4.1.2021.8.1.2.108.100.1 = INTEGER: 0
iso.3.6.1.4.1.2021.8.1.2.108.101.1 = STRING:
"system.@system[0].config_description=Version 1.1 Beta ABC"
iso.3.6.1.4.1.2021.8.1.2.108.102.1 = INTEGER: 0
iso.3.6.1.4.1.2021.8.1.2.108.103.1 = ""
```

Commit this change from UCI temporary storage to permanent overlay file system.

```
snmpset -c private -v 2c 192.168.100.1 1.3.6.1.4.1.2021.8.1 s "uci
commit system"
```

No service reload is required.

7.7.3.3 Delete system configuration description text

The following command sequence

```
snmpset -c private -v 2c 192.168.100.1 1.3.6.1.4.1.2021.8.1 s "uci
delete system.@system[0].config_description"
```

snmpwalk -c public -v 2c 192.168.100.1 1.3.6.1.4.1.2021.8.1.2.108

delivers

```
iso.3.6.1.4.1.2021.8.1.2.108.1.1 = INTEGER: 1
iso.3.6.1.4.1.2021.8.1.2.108.2.1 = STRING: "uci_get"
iso.3.6.1.4.1.2021.8.1.2.108.3.1 = STRING: "/usr/sbin/get_snmp
uci_get"
iso.3.6.1.4.1.2021.8.1.2.108.100.1 = INTEGER: 0
iso.3.6.1.4.1.2021.8.1.2.108.101.1 = STRING: "uci: Entry not found"
iso.3.6.1.4.1.2021.8.1.2.108.101.2 = STRING:
"system.@system[0].config_description="
iso.3.6.1.4.1.2021.8.1.2.108.102.1 = INTEGER: 0
iso.3.6.1.4.1.2021.8.1.2.108.103.1 = ""
```

Commit this change from UCI temporary storage to permanent overlay file system.

```
snmpset -c private -v 2c 192.168.100.1 1.3.6.1.4.1.2021.8.1 s "uci commit system"
```

7.8 SNMP Applications

7.8.1 SNMP Support for GPS

The following information data structure can be obtained via SNMP command 'snmpwalk' from a host system.

The command

ELTEC

user@host:~\$ snmpwalk -c public -v2c 192.168.100.1 1.3.6.1.4.1.2021.8.1.2.155

delivers

iso.3.6.1.4.1.2021.8.1.2.155.1.1 = INTEGER: 1 iso.3.6.1.4.1.2021.8.1.2.155.2.1 = STRING: "gps_info" iso.3.6.1.4.1.2021.8.1.2.155.3.1 = STRING: "/bin/cat /var/run/gps/gps.info" iso.3.6.1.4.1.2021.8.1.2.155.100.1 = INTEGER: 0 iso.3.6.1.4.1.2021.8.1.2.155.101.1 = STRING: "Status: A" iso.3.6.1.4.1.2021.8.1.2.155.101.2 = STRING: "Quality: 1" iso.3.6.1.4.1.2021.8.1.2.155.101.3 = STRING: "Sat: 9" iso.3.6.1.4.1.2021.8.1.2.155.101.4 = STRING: "Wed Jul 5 09:45:15 2017" iso.3.6.1.4.1.2021.8.1.2.155.101.5 = STRING: "N: 49.960107" iso.3.6.1.4.1.2021.8.1.2.155.101.6 = STRING: "E: 8.258518" iso.3.6.1.4.1.2021.8.1.2.155.101.7 = Hex-STRING: 4E 3A 20 34 39 C2 B0 35 37 27 33 36 2E 33 38 34 2.2 iso.3.6.1.4.1.2021.8.1.2.155.101.8 = Hex-STRING: 45 3A 20 38 C2 B0 31 35 27 33 30 2E 36 36 36 22 iso.3.6.1.4.1.2021.8.1.2.155.101.9 = STRING: "Alt: 175.75m" iso.3.6.1.4.1.2021.8.1.2.155.101.10 = STRING: "Speed: 1 km/h" iso.3.6.1.4.1.2021.8.1.2.155.101.11 = "" iso.3.6.1.4.1.2021.8.1.2.155.102.1 = INTEGER: 0 iso.3.6.1.4.1.2021.8.1.2.155.103.1 = ""

The values "Latitude DMS" and "Longitude DMS" are returned as Hex strings because they contain quote and double quotes.

This converted NMEA 0183 data struct is supplied with default configuration (after factory reset). The configuration can be adapted to supply the raw NMEA 0183 protocol. Following steps are necessary to switch over to raw protocol.

Open a remote root console with 'ssh' access and apply following commands.

```
root@CyBoxAP:/# uci set system.@gps[0].raw='1'
root@CyBoxAP:/# uci commit
root@CyBoxAP:/# reboot
```

After reboot the GPS subsystem is configured to supply raw NMEA 0183 data. Note that this data is not shown in web interface, but can be readout via SNMP (different OID than converted GPS info).

The command

```
user@host:~$ snmpwalk -c public -v2c 192.168.100.1 1.3.6.1.4.1.2021.8.1.2.156
```

will return

```
iso.3.6.1.4.1.2021.8.1.2.156.1.1 = INTEGER: 1
iso.3.6.1.4.1.2021.8.1.2.156.2.1 = STRING: "gps_raw"
iso.3.6.1.4.1.2021.8.1.2.156.3.1 = STRING: "/bin/cat
/var/run/gps/gps.raw"
iso.3.6.1.4.1.2021.8.1.2.156.100.1 = INTEGER: 0
iso.3.6.1.4.1.2021.8.1.2.156.101.1 = STRING:
"$GPRMC,094908.000,A,4957.5942,N,00815.4955,E,0.2,194.2,050717,,,A\*6E"
iso.3.6.1.4.1.2021.8.1.2.156.101.2 = STRING:
"$GPGGA,094908.000,4957.5942,N,00815.4955,E,1,07,1.3,149.90,M,47.9,M,,\*6E"
iso.3.6.1.4.1.2021.8.1.2.156.101.3 = STRING:
"$GNGSA,A,3,24,25,32,29,31,02,,,,,,,2.2,1.3,1.8\*2C"
iso.3.6.1.4.1.2021.8.1.2.156.101.4 = STRING:
"$GNGSA,A,3,77,,,,,,,,,,,2.2,1.3,1.8\*27"
iso.3.6.1.4.1.2021.8.1.2.156.101.5 = STRING:
"$GPGSV,3,1,10,02,39,076,17,06,13,033,,12,40,086,13,14,30,267,\*7F"
iso.3.6.1.4.1.2021.8.1.2.156.101.6 = STRING:
"$GPGSV,3,2,10,24,12,151,34,25,79,051,21,26,02,280,,29,61,213,25\*77"
iso.3.6.1.4.1.2021.8.1.2.156.101.7 = STRING:
"$GPGSV,3,3,10,31,40,305,25,32,22,244,32,,,,,,,\*7D"
iso.3.6.1.4.1.2021.8.1.2.156.101.8 = STRING:
"$GLGSV,2,1,07,81,19,201,,70,11,350,,77,42,124,33,79,34,317,\*6F"
iso.3.6.1.4.1.2021.8.1.2.156.101.9 = STRING:
"$GLGSV,2,2,07,69,08,297,,88,69,171,,87,52,044,,,,\*59"
iso.3.6.1.4.1.2021.8.1.2.156.102.1 = INTEGER: 0
iso.3.6.1.4.1.2021.8.1.2.156.103.1 = ""
```

7.8.2 SNMP Support for Second GPS Source

On some CyBox AP models the LTE modem can also provide additional GPS information. If the modem GPS is activated, and an additional GPS antenna is plugged in, these SNMP OIDs can be used to gather the additional GPS information.

gps_module0_info	1.3.6.1.4.1.2021.8.1.2.157
gps_module0_raw	1.3.6.1.4.1.2021.8.1.2.158
gps_module1_info	1.3.6.1.4.1.2021.8.1.2.159
gps_module1_raw	1.3.6.1.4.1.2021.8.1.2.160

8 THE FLYING CONTROLLER MECHANISM

Some tasks require knowledge which is not available at a single network node. For example, to detect a "rogue access point", all access points belonging to the WLAN network must be known, in order to identify those who don't. Also, multiple access points scan the vicinity, and their results have to be collected and evaluated at one central point. Therefore a single "controller" is needed in the network which collects those information and then performs the rogue AP detection.

The "flying controller" is an algorithm which runs on multiple network devices simultaneously and which elects one of these devices as the "controller". All other devices are called "workers". If the controller fails, a new one is elected, hence the term "flying". This way, a central controller is established without creating a single point of failure.

The CyBox AP 3 automatically takes part on the mechanism and could be elected as controller, or otherwise will be a worker.

The election mechanism is the foundation for the 6.1.2.12 Rogue Access Point Detection Service . This service runs on the controller and collects data from the workers to detect rogue APs.

The flying controller mechanism has no configuration options.

9 IPSecVPN / StrongSwan

strongSwan is a multiplatform IPsec implementation. The focus of the project is on strong authentication mechanisms using X.509 public key certificates and optional secure storage of private keys and certificates on smartcards through a standardized PKCS#11 interface and on TPM 2.0.

Detailed information about the **strongSwan IPsec** implementation can be found here:

https://www.strongswan.org/about.html

https://wiki.strongswan.org/projects/strongswan

9.1 IPSec Customized Configuration

The implementation of the IPSecVPN LuCi web interface and the OpenWrt service startup is to generate three service conform config files out of the OpenWrt configuration file '*/etc/config/ipsec*'.

These three standard configuration files are:

- IPSEC_SECRETS_FILE=/etc/ipsec.secrets
- IPSEC_CONN_FILE=/etc/ipsec.conf
- STRONGSWAN_CONF_FILE=/etc/strongswan.conf

When IPSec service is started, the configuration file '/etc/config/ipsec' is converted into three volatile config include files located in '/var/ipsec/'

- IPSEC_VAR_SECRETS_FILE=/var/ipsec/ipsec.secrets
- IPSEC_VAR_CONN_FILE=/var/ipsec/ipsec.conf
- STRONGSWAN_VAR_CONF_FILE=/var/ipsec/strongswan.conf

The three standard configuration files do include the generated files, but may also be adapted on the IPSecVPN web page with the corresponding menu editor.

Chatua		
Status	Connection Status General Configuration Edit "ipsec.conf Edit "ipsec.secrets' Edit "strongswan.conf	
System	Edit 'ipsec.conf'	
VPN	This is the content of //etc/ipsec.conf, the main configuration file for ipsec service.	
IPSecVPN	# ipsec.conf - strongSwan IPsec configuration file	
OpenVPN		
Services	# basic configuration	
Network	<pre>config setup # strictrlpolicy=yes # uniqueids = no</pre>	
Statistics	# Add connections here.	
Logout	# Sample VPN connections #conn sample-self-signed	
	<pre># leftsubnet=10.1.0.0/16 # leftcert=selfCert.der</pre>	
	<pre># leftsendcert=never # right=192.168.0.2</pre>	
	<pre># rightsubnet=10.2.0.0/16 # rightcert=peerCert.der</pre>	
	# auto=start	
	#conn sample-with-ca-cert # leftsubnet=10.1.0.0/16	
	<pre># leftcert=myCert.pem # right=192.168.0.2</pre>	
	# rightsubnet=10.2.0.0/16	
	<pre># rightid="C=CH, 0=Linux strongSwan CN=peer name" #uto=start</pre>	
	include /var/ipsec/ipsec.conf	lh.
	Submit	Reset

ELTEC

systems

IPSec service configuration files can be edited (customized)

9.2 IPSec default configuration

The service is disabled in default factory configuration. First step is to decide if configuration files should be automatically generated or are provided and edit by operator. The next chapters supposes that configuration is generated by IPSec start script (init.d/ipsec).

System IPSec-Strongswan VPN VPN General Configuration IPSecVPN Enable service OpenVPN Enable service Generate config files @ Enable automatic generation of IPSec configuration files	
IPSecVPN General Configuration OpenVPN Enable service Generate config files Image: Configuration of IPSec configuration files	
OpenVPN Enable service Image: Control of the service Services Generate config files Image: Control of the service	
Services Generate config files Generation of IPSec configuration files	
Contract Contract	
Network Debug level	
Stausucs	
Install routing tables	
Logout Ignore routing tables	
Interface List	
Secret Configuration	
This section contains no values yet	
Add	
Tunnel Connections	
This section contains no values yet	
bbA	
Transport Connections	
This section contains no values yet	
Add	
Crypto Proposals	
	Delete
CP_1	
Encryption Algorithm aes256	
Hash Algorithm sha256	
DH Group modp2048	
Force crypto proposal	

IPSec factory default configuration

9.3 IPSec Secret configuration

The ipsec.secrets file keeps the Pre-Shared-Keys (*PSK*) for a prior configured Tunnel and/or Transport connection. The *PSK* is the one and only supported authentication method.

IY_SEC		De
Enabled	✓	
Gateway	192.168.100.15	
Pre Shared Key		
Authentication method	psk _	
Local identifier	192.168.100.14	
Remote identifier	192.168.100.15	
Tunnel Connection	my_tun ×	
	+	
Transport Connection	+	

PSK Secret configuration

9.4 IPSec Tunnel / Transport Connection

The parameters in this menu are named analogue to the standard parameters in offical configuration documentation. Please refer to:

https://wiki.strongswan.org/projects/strongswan/wiki/ConfigurationFiles

		Delete
MY_TUN		
Mode	start	
	Mode for option 'auto'	
Local subnet	10.1.0.0/16	
Local NAT		
Local source IP	192.168.100.14	
Local UpDown		
Local firewall		
Remote subnet	10.2.0.0/16	
Remote source IP	192.168.100.15	
Remote UpDown		
Remote firewall		
IKE life time	3h	
Lifetime	1h	
Margintime	9m	
Keying tries	3	
DPD action	none	
DPD delay	30s	
Inactivity		
Key exchange	ikev2 👻	
ReqID		
IKE Proposal	cp_1 *	
	*	
ESP Proposal	cp_5 ×	
Add		

Tunnel Connection configuration

The Transport Connection is similar to the Tunnel Connection setup.

	Transport Connections This section contains no values yet	
	Add	

Transport Connection configuration

9.5 IPSec Crypto Proposal configuration

In default factory configuration some Crypto Proposal are already defined. With the Add button new proposals can be added. Use the Delete button to remove unneeded Crypto Proposals from configuration.

CP_1		D
Encryption Algorithm	aes256	
Hash Algorithm	sha256	
DH Group	modp2048	
Force crypto proposal		
		D
P_2		
r_z		
	aes256gmac	
Encryption Algorithm	aes256gmac sha256	
Encryption Algorithm Hash Algorithm DH Group		

Crypto Proposals, some are predefined

9.6 IPSec Firewall Custom Rules

The standard firewall setup (factory default) may require new custom rules to handle IPSec ESP package forwarding.

Status	General Settings Port Forwards Traffic Rules Custom Rules	
System	Firewall - Custom Rules	
VPN	Custom rules allow you to execute arbitrary iptables commands which are not otherwise covered by the firewall framework. The commands	
Services	are executed after each firewall restart, right after the default ruleset has been loaded.	
Network	<pre># This file is interpreted as shell script. # Put your custom iptables rules here, they will</pre>	
Interfaces	# be executed with each firewall (re-)start.	
DHCP and DNS	# Internal uci firewall chains are flushed and recreated on reload, so	
Hostnames	<pre># put custom rules into the root chains e.g. INPUT or FORWARD or into the # special user chains, e.g. input_wan_rule or postrouting_lan_rule.</pre>	
Static Routes	iptables -I INPUT -m policydir inpol ipsecproto esp -j ACCEPT	
Diagnostics	iptables -I FORWARD -m policydir inpol ipsecproto esp -j ACCEPT iptables -I FORWARD -m policydir outpol ipsecproto esp -i ACCEPT	
Firewall	iptables -I OUTPUT -m policydir outpol ipsecproto esp -j ACCEPT	
Client Isolation		
Connection Check		
QoS		
Configure Diagnostics		
Load Balancing		
Statistics	Restart Firewall Reset	
Logout		

The firewall obtained some additional custom rules

Cut and Paste buffer for IPSec Firewall - Custom Rules edit:

iptables -I INPUT -m policy --dir in --pol ipsec --proto esp -j ACCEPT iptables -I FORWARD -m policy --dir in --pol ipsec --proto esp -j ACCEPT iptables -I FORWARD -m policy --dir out --pol ipsec --proto esp -j ACCEPT iptables -I OUTPUT -m policy --dir out --pol ipsec --proto esp -j ACCEPT

9.7 IPSec Service Start

If the Enable service box is activated and new settings are applied, the service will restart.

Status	Connection Status General Configuration Edit 'ipsec.conf	Edit 'ipsec.secrets' Edit 'strongswan.conf	
System	IPSec-Strongswan VPN		
VPN	General Configuration		
IPSecVPN			
OpenVPN	Enable service		
Services	Generate config files		
Network	e Enable automatic generation of IPSec configuration files		
Statistics	Debug level	0	
	Install routing tables		
Logout	Ignore routing tables	0	
	Interface List	lan ×	
		+	

IPSec service is automatically restarted

The IPSec service connection status can ob observed in the Connection Status menu tab.

Status	Connection Status General Configuration Edit "ipsec.conf" Edit "ipsec.secrets" Edit 'strongswan.conf
System	Connection Status
VPN	
IPSecVPN	uptime: 7 seconds, since Apr 08 11:06:28 2020 malloc: sbrk 679936, mmap 0, used 187264, free 492672
OpenVPN	worker threads: 11 of 16 idle, 5/0/0/0 working, job queue: 0/0/0/0, scheduled: 1 loaded plugins: charon aes des rc2 sha2 sha1 md5 random nonce x509 revocation constraints pubkev pkcs1 pgp dnskev sshkev pem fi
Services	Virtual IP pools (size/online/offline): 192.168.100.15: 1/0/0
Network	Listening IP addresses: 192.168.100.1
Statistics	10.13.18.229 192.168.3.151 10.4.215.228 fd5d:69f4.7983::1
Logout	Connections: my_sec-my_tun: %any192.168.100.15 IKEv2 my_sec-my_tun: local: [192.168.100.14] uses pre-shared key authentication my_sec-my_tun: remote: [192.168.100.15] uses pre-shared key authentication my_sec-my_tun: remote: [192.168.100.15] uses pre-shared key authentication my_sec-my_tun: remote: [192.168.100.15] uses pre-shared key authentication my_sec-my_tun: remote: [192.168.100.16.016] Security Associations (0 up, 1 connecting): my_sec-my_tun[1]: ONNECTING, 192.168.100.1[%any]192.168.100.15[%any] my_sec-my_tun[1]: IKEV2 SPIs: 487d5fbe090542cb i* 00000000000000 r my_sec-my_tun[1]: Tasks active: IKE_VENDOR IKE_INIT IKE_NATD IKE_CERT_PRE IKE_AUTH IKE_CERT_POST IKE_CONFIG CHILD_CREATE IKE_AUTH my_sec-my_tun[1]: Tasks active: IKE_VENDOR IKE_INIT IKE_NATD IKE_CERT_PRE IKE_AUTH IKE_CERT_POST IKE_CONFIG CHILD_CREATE IKE_AUTH

Status of IPSec service waiting for connection

10 SSH / SERIAL CONSOLE

On a Windows PC, you can use the program PuTTY (http://www.putty.org).

a. Ethernet cable (SSH)

Ensure that an Ethernet cable is connected between your PC and the access point. The following instruction assumes that the default settings are used.

- If you are using a UNIX/Linux PC then run the command 'ssh root@192.168.100.1'.
- If you are using a Windows PC, PuTTY should be configured as follows:

Basic options for your PuTTY ses	sion	
Specify the destination you want to connect to		
Host Name (or IP address) Port		
192.168.100.1 22		
Connection type: ◯ Raw ◯ Telnet ◯ Rlogin ⓒ SSH	Serial	

PuTTY - SSH connection

b. Serial cable

Ensure that a serial cable is connected between your PC and the access point (a specific CyBox adapter plugged in the USB port is required).

- On a UNIX PC, install the program picocom, and run command picocom -b 115200 /dev/ttyUSB0 (*'ttyUSB0'* must be modified depending on your PC).
- If you are using a Windows PC, PuTTY should be configured as follows:

Basic options for your PuTTY session		
Specify the destination you want to connect to		
Serial line	Speed	
COM11	115200	
Connection type:	Serial	

PuTTY - Serial connection

The value 'COM11' must be adapted for your PC. A list of the COM ports can be found in the device manager window as shown below.

🚔 Geräte-Manager
Datei Aktion Ansicht ?
FE-VM-WIN7
a 🐺 Anschlüsse (COM & LPT)
📲 Intel(R) Active Management Technology - SOL (COM3)
USB Serial Port (COM11)
Audio-, Video- und Gamecontroller
⊳ - 🖳 Computer
N® DVD/CD-ROM-Laufwerke
Windows dovice manager showing COM ports

Windows device manager showing COM ports

Once the connection is established, a login should be requested on serial console window.

If this is not the case, press Enter on the keyboard and/or disconnect and reconnect the USB serial adapter on the CyBox side. To edit files on target system the build-in text editor **nano** can be used.

10.1 UCI Configuration

This section describes the UCI (**Unified Configuration Interface**). UCI can be scripted for remote configuration using shell commands and scripts. UCI can be seen as the OpenWRT main configuration interface. It is best used for main network interface configuration, wireless settings, logging functionality and remote access configuration.

With OpenWrt, the user should change only UCI configuration file(s), which are read by individual programs.

For a more complete description of UCI commands and files used see https://wiki.openwrt.org/doc/uci.

10.1.1 UCI configuration files

The OpenWRT central configuration is split into several files located in the /etc/config/ directory. Each file is named according to the part of the system it configures. The configuration files can either be modified using a text editor or by using UCI. UCI configuration files are also modifiable through various programming APIs (like Shell, Lua and C), which is also how web interfaces like LuCI make changes to the UCI files.

After changing a UCI configuration file, the services affected must be restarted by an init.d call, so the updated UCI configuration is used. Many programs are made compatible with UCI by making their init.d script write their standard program-specific configuration files. The init.d script first writes the configuration file to the location expected by the software and it is read in again by restarting the executable. Note that just (re)starting the executable directly, without init.d calls, will not result in an UCI update. Changes in files in /etc/config/ then take no effect.

10.1.2 UCI Example

As an example, suppose you want to change the device's IP address from the default 192.168.100.1 to 192.168.2.1. Change the line in the file /etc/config/network:

option ipaddr 192.168.100.1

to:

```
option ipaddr 192.168.2.1
```

Next, commit the settings by running:

/etc/init.d/network restart

Remember to login again to the new IP address.

10.2 Other commands

a. Restore factory settings

The factory settings can be restored with the command factory_reset

b. Export configuration

The current configuration can be saved in the CyBox folder '/*tmp*/' with the command sysupgrade -b /tmp/backup<mybackupname>.tar.gz. It can then be exported to a PC with SCP (or the program WinSCP for Windows).

c. Import configuration

Restore the factory settings and then import your archived configuration to '/*tmp*/' with SCP (or WinSCP), the configuration can be installed with the command sysupgrade -r /tmp/backup-<mybackupname>.tar.gz ; reboot

Typing reboot in the command line will reboot the device.

USB stick is auto-mounted to /mnt/sda1.

11 SYSTEM MAINTENANCE

11.1 Remote Firmware Upgrade

The *standard_boot* flash partition, which contains the standard firmware binary image (.itb image), can be updated remotely. The new firmware image must be copied to the target system with **scp** command. Afterwards **ssh** calls will execute local target programs to install the new firmware.

While OpenWrt operating system is running, the standard_boot partition can be written at any time.

If firmware update does **not** require a configuration change, the current system configuration can be kept. Please contact support or sales department if a configuration reset is needed for your update purpose from an older version to a newer one.

The **Appendix: Script for Remote Firmware Update** provides a *Bash* script **rsysupgrade.sh** to demonstrate the remote update process from a Linux Host console.

11.1.1 Remote Firmware Upgrade without Config Change

Normally a firmware update should also include a configuration reset to the new version. Only in some few cases e.g. a small bug fix on a wireless driver, will not require to adapt and install a new configuration backup archive.

The following commands may be executed from a Linux console or with similar Windows **Putty** utils.

1. Copy the new firmware image to the target system

scp <new_firmware.itb> root@<target_ipv4>:/tmp/firmware.img

2. Flash new firmware to the standard_boot flash partition (mtd2) and reboot the target system

ssh root@<target_ipv4>: "/sbin/sysupgrade -t /tmp/firmware.img; reboot"

11.1.2 Remote Firmware Upgrade with New Config

In most cases an adapted or new configuration archive must also be installed, to match the new firmware version. The overlay partition is used to keep the configuration settings made by user to be present after power cycle. If the firmware detects an empty (cleared) overlay partition, the target directory /mnt/custom/ is checked for a single **backup-<target>-<cfg>.tar.gz** archive to be installed as a new configuration. If a /mnt/custom/backup-<target>-<cfg>.tar.gz archive does not exist, the factory default settings are applied.

To create your custom configuration for a new firmware, the old system firmware should be updated to the new version with deleted configuration and factory settings applied. Make your complete system configuration setup with the new firmware version and save the **backup-<target>-<cfg>.tar.gz** archive to your Host System. The uploaded backup archive can then be exported to other (stationary) targets with the same hardware components equipped.

The following commands may be executed from a Linux console or with similar Windows **Putty** utils.

1. Copy the new firmware image to the target system

```
scp <new_firmware.itb> root@<target_ipv4>:/tmp/firmware.img
```

- 2. Flash new firmware to the **standard_boot** flash partition (mtd2)
 - ssh root@<target_ipv4>: "/sbin/sysupgrade -t /tmp/firmware.img"
- 3. Ensure that no backup configuration is stored in /mnt/custom/
 - ssh root@<target_ipv4>: "rm -rf /mnt/custom/backup*"
- 4. Optionally, export your new custom configuration to /mnt/custom/. Note that the target system will perform a extra reboot cycle, to activate your new configuration setup. If no configuration is exported, the default configuration of the new firmware will automatically be applied.

scp backup-<my_config>.tar.gz root@/<target_ipv4>:/mnt/custom/

5. Delete the current configuration and reboot:

ssh root@<target_ipv4>: "rm -rf /mnt/jffs2/*; reboot"

WARNING: Do NOT POWER OFF the access point while upgrading/restoring firmware to flash

11.2 USB Possibilities

Via USB stick it is possible to update configuration and firmware.

A USB stick can be connected to the device, it needs a dedicated USB adapter.

a. Export configuration

Archived configurations can be exported from the command line to an empty USB stick by copying the configuration to '*/mnt/sda1*'.

b. Import configuration

To import an archived configuration to the access point, wait until booting is completed, then connect a USB stick with a configuration file on it named like '*backup-<mycustomname>.tar.gz*' No other file or folder must be present on the stick. Once plugged in, the configuration will be automatically read in and two reboots will successively happen in order to apply your settings. The USB stick can safely be removed at the beginning of a boot phase (when all LEDs are turned off), or when the boot sequence is completed.

A USB hotplug script is triggered if the USB stick is plugged in after booting. It reads the root directory of the stick and checks for a list of known file types:

Files on upgrade USB stick:

File Type (wildcard=*)	Description	Board	Action	Who ?
"backup*tar.gz"	New configuration archive	ALL	Untar to Overlay FS (/dev/mtd3)	End user
"factory*reboot"	Marker to do a factory reset and reboot after upgrade operation.	ALL	Execute factory_reset	End user
"config*reboot"	Marker to do a perform a normal reboot.	ALL	Execute reboot	End user
"cyap*upgrade*tgz" "cyap*upgrade*zip"	Upgrade archive must contain an 'install.sh' script (executable) in archive root. The archive is unpacked to /tmp/usb_upgrade and 'install.sh' is executed.	ALL	Shell script execution	System Integrator

Every install is executed only once for each file on the USB stick; updates already installed are not tried again. Check '*System Log*' in web interface or logread on console for upgrade messages.

For a firmware upgrade with *.zip archive the USB stick should only provide one archive file in USB root directory:

Example:

cyap-upgrade-V20.36.3.zip

This upgrade archive file must contain the new *V20.36.3-cyap2-lzma.itb* firmware image and an executable install script named *install.sh*. The install script executes commands to flash the new firmware into the desired partition. The upgrade archive may also include a new configuration backup archive, suitable for the new firmware version. After firmware upgrade, the new configuration may also applied with commands from the install script.

Example for an *install.sh* script:

ELTEC systems

#!/bin/sh	
1 10	V20.36.3-cyap2-lzma.itb backup-cyap2-20.36.3.tar.gz
exit O	

11.3 Status LED Blink Codes

While the upgrade process is running or has finished the 'Fail LED' (red/green) is used as status indicator. Blink codes in upgrades:

Blink Code repeated	Description
RED 0.2sec on - GREEN 0.2sec on	Upgrade process running
GREEN continuous on	Upgrade successful
RED continuous on	USB stick mount failed
RED 3sec on - OFF 0.5sec	Mount of overlay FS failed
GREEN 3sec on – OFF 0.5sec	Some Upgrade is already one
RED 0.2sec – OFF 0.5sec – RED 0.2sec – OFF 2sec	Copy to flash failed
RED 0.2sec – OFF 0.5sec – RED 0.2sec – OFF 0.5sec – RED 0.2sec OFF 2sec	'install.sh' missing
GREEN 0.2sec – OFF 0.5sec – RED 0.2sec – OFF 0.5sec – RED 0.2sec - OFF 0.5sec	Password missing
GREEN 0.2sec – OFF 0.5sec – RED 0.2sec – OFF 0.5sec – RED 0.2sec - OFF 0.5sec – RED 0.2sec - OFF 0.5sec	Password invalid
OFF	USB stick is removed

12 APPENDIX: GPL LICENSE

GNU GENERAL PUBLIC LICENSE

Version 3, 29 June 2007

Copyright © 2007 Free Software Foundation, Inc. <https://fsf.org/>

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

PREAMBLE

The GNU General Public License is a free, copyleft license for software and other kinds of works.

The licenses for most software and other practical works are designed to take away your freedom to share and change the works. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change all versions of a program--to make sure it remains free software for all its users. We, the Free Software Foundation, use the GNU General Public License for most of our software; it applies also to any other work released this way by its authors. You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for them if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs, and that you know you can do these things.

To protect your rights, we need to prevent others from denying you these rights or asking you to surrender the rights. Therefore, you have certain responsibilities if you distribute copies of the software, or if you modify it: responsibilities to respect the freedom of others.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must pass on to the recipients the same freedoms that you received. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

Developers that use the GNU GPL protect your rights with two steps: (1) assert copyright on the software, and (2) offer you this License giving you legal permission to copy, distribute and/or modify it.

For the developers' and authors' protection, the GPL clearly explains that there is no warranty for this free software. For both users' and authors' sake, the GPL requires that modified versions be marked as changed, so that their problems will not be attributed erroneously to authors of previous versions.

Some devices are designed to deny users

access to install or run modified versions of the software inside them, although the manufacturer can do so. This is fundamentally incompatible with the aim of protecting users' freedom to change the software. The systematic pattern of such abuse occurs in the area of products for individuals to use, which is precisely where it is most unacceptable. Therefore, we have designed this version of the GPL to prohibit the practice for those products. If such problems arise substantially in other domains, we stand ready to extend this provision to those domains in future versions of the GPL, as needed to protect the freedom of users.

Finally, every program is threatened constantly by software patents.

States should not allow patents to restrict development and use of software on general-purpose computers, but in those that do, we wish to avoid the special danger that patents applied to a free program could make it effectively proprietary. To prevent this, the GPL assures that patents cannot be used to render the program non-free.

ELTEC

systems

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS

0. Definitions.

"This License" refers to version 3 of the GNU General Public License.

"Copyright" also means copyright-like laws that apply to other kinds of works, such as semiconductor masks.

"The Program" refers to any copyrightable work licensed under this License. Each licensee is addressed as "you". "Licensees" and "recipients" may be individuals or organizations.

To "modify" a work means to copy from or adapt all or part of the work in a fashion requiring copyright permission, other than the making of an exact copy. The resulting work is called a "modified version" of the earlier work or a work "based on" the earlier work.

A "covered work" means either the unmodified Program or a work based on the Program.

To "propagate" a work means to do anything with it that, without permission, would make you directly or secondarily liable for infringement under applicable copyright law, except executing it on a computer or modifying a private copy. Propagation includes copying, distribution (with or without modification), making available to the public, and in some countries other activities as well.

To "convey" a work means any kind of propagation that enables other parties to make or receive copies. Mere interaction with a user through a computer network, with no transfer of a copy, is not conveying.

An interactive user interface displays "Appropriate Legal Notices" to the extent that it includes a convenient and prominently visible feature that (1) displays an appropriate copyright notice, and (2) tells the user that there is no warranty for the work (except to the extent that warranties are provided), that licensees may convey the work under this License, and how to view a copy of this License. If the interface presents a list of user commands or options, such as a menu, a prominent item in the list meets this criterion.

1. Source Code.

The "source code" for a work means the preferred form of the work for making modifications to it. "Object code" means any non-source form of a work.

A "Standard Interface" means an interface that either is an official standard defined by a recognized standards body, or, in the case of interfaces specified for a particular programming language, one that is widely used among developers working in that language.

The "System Libraries" of an executable work include anything, other than the work as a whole, that (a) is included in the normal form of packaging a Major Component, but which is not part of that Major Component, and (b) serves only to enable use of the work with that Major Component, or to implement a Standard Interface for which an

ELTEC

implementation is available to the public in source code form. A "Major Component", in this context, means a major essential component (kernel, window system, and so on) of the specific operating system (if any) on which the executable work runs, or a compiler used to produce the work, or an object code interpreter used to run it.

The "Corresponding Source" for a work in object code form means all the source code needed to generate, install, and (for an executable work) run the object code and to modify the work, including scripts to control those activities. However, it does not include the work's System Libraries, or general-purpose tools or generally available free programs which are used unmodified in performing those activities but which are not part of the work. For example, Corresponding Source includes interface definition files associated with source files for the work, and the source code for shared libraries and dynamically linked subprograms that the work is specifically designed to require, such as by intimate data communication or control flow between those subprograms and other parts of the work.

The Corresponding Source need not include anything that users can regenerate automatically from other parts of the Corresponding Source.

The Corresponding Source for a work in source code form is that same work.

2. Basic Permissions.

All rights granted under this License are granted for the term of copyright on the Program, and are irrevocable provided the stated conditions are met. This License explicitly affirms your unlimited permission to run the unmodified Program. The output from running a covered work is covered by this License only if the output, given its content, constitutes a covered work. This License acknowledges your rights of fair use or other equivalent, as provided by copyright law.

You may make, run and propagate covered works that you do not convey, without conditions so long as your license otherwise remains in force. You may convey covered works to others for the sole purpose of having them make modifications exclusively for you, or provide you with facilities for running those works, provided that you comply with the terms of this License in conveying all material for which you do not control copyright. Those thus making or running the covered works for you must do so exclusively on your behalf, under your direction and control, on terms that prohibit them from making any copies of your copyrighted material outside their relationship with you.

Conveying under any other circumstances is permitted solely under the conditions stated below. Sublicensing is not allowed; section 10 makes it unnecessary.

3. Protecting Users' Legal Rights From Anti-Circumvention Law.

No covered work shall be deemed part of an effective technological measure under any applicable law fulfilling obligations under article 11 of the WIPO copyright treaty adopted on 20 December 1996, or similar laws prohibiting or restricting circumvention of such measures.

When you convey a covered work, you waive any legal power to forbid circumvention of technological measures to the extent such circumvention is effected by exercising rights under this License with respect to the covered work, and you disclaim any intention to limit operation or modification of the work as a means of enforcing, against the work's users, your or third parties' legal rights to forbid circumvention of technological measures.

4. Conveying Verbatim Copies.

You may convey verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice; keep intact all notices stating that this License and any non-permissive terms added in accord with section 7 apply to the code; keep intact all notices of the absence of any warranty; and give all recipients a copy of this License along with the Program.

ELTEC

systems

You may charge any price or no price for each copy that you convey, and you may offer support or warranty protection for a fee.

5. Conveying Modified Source Versions.

You may convey a work based on the Program, or the modifications to produce it from the Program, in the form of source code under the terms of section 4, provided that you also meet all of these conditions:

a) The work must carry prominent notices stating that you modified it, and giving a relevant date. b) The work must carry prominent notices stating that it is released under this License and any conditions added under section 7. This requirement modifies the requirement in section 4 to "keep intact all notices". c) You must license the entire work, as a whole, under this License to anyone who comes into possession of a copy. This License will therefore apply, along with any applicable section 7 additional terms, to the whole of the work, and all its parts, regardless of how they are packaged. This License gives no permission to license the work in any other way, but it does not invalidate such permission if you have separately received it. d) If the work has interactive user interfaces, each must display Appropriate Legal Notices; however, if the Program has interactive interfaces that do not display Appropriate Legal Notices, your work need not make them do so.

A compilation of a covered work with other separate and independent works, which are not by their nature extensions of the covered work, and which are not combined with it such as to form a larger program, in or on a volume of a storage or distribution medium, is called an "aggregate" if the compilation and its resulting copyright are not used to limit the access or legal rights of the compilation's users beyond what the individual works permit. Inclusion of a covered work in an aggregate does not cause this License to apply to the other parts of the aggregate.

6. Conveying Non-Source Forms.

You may convey a covered work in object code form under the terms of sections 4 and 5, provided that you also convey the machine-readable Corresponding Source under the terms of this License, in one of these ways:

a) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by the Corresponding Source fixed on a durable physical medium customarily used for software interchange. b) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by a written offer, valid for at least three years and valid for as long as you offer spare parts or customer support for that product model, to give anyone who possesses the object code either (1) a copy of the Corresponding Source for all the software in the product that is covered by this License, on a durable physical medium customarily used for software interchange, for a price no more than your reasonable cost of physically performing this conveying of source, or (2) access to copy the Corresponding Source from a network server at no charge. c) Convey individual copies of the object code with a copy of the written offer to provide the Corresponding Source. This alternative is allowed only occasionally and noncommercially, and only if you

received the object code with such an offer, in accord with subsection 6b. d) Convey the object code by offering access from a designated place (gratis or for a charge), and offer equivalent access to the Corresponding Source in the same way through the same place at no further charge. You need not require recipients to copy the Corresponding Source along with the object code. If the place to copy the object code is a network server, the Corresponding Source may be on a different server (operated by you or a third party) that supports equivalent copying facilities, provided you maintain clear directions next to the object code saying where to find the Corresponding Source. Regardless of what server hosts the Corresponding Source, you remain obligated to ensure that it is available for as long as needed to satisfy these requirements. e) Convey the object code using peer-to-peer transmission, provided you inform other peers where the object code and Corresponding Source of the work are being offered to the general public at no charge under subsection 6d.

ELTEC

systems

A separable portion of the object code, whose source code is excluded from the Corresponding Source as a System Library, need not be included in conveying the object code work.

A "User Product" is either (1) a "consumer product", which means any tangible personal property which is normally used for personal, family, or household purposes, or (2) anything designed or sold for incorporation into a dwelling. In determining whether a product is a consumer product, doubtful cases shall be resolved in favor of coverage. For a particular product received by a particular user, "normally used" refers to a typical or common use of that class of product, regardless of the status of the particular user or of the way in which the particular user actually uses, or expects or is expected to use, the product. A product is a consumer product regardless of whether the product has substantial commercial, industrial or non-consumer uses, unless such uses represent the only significant mode of use of the product.

"Installation Information" for a User Product means any methods, procedures, authorization keys, or other information required to install and execute modified versions of a covered work in that User Product from a modified version of its Corresponding Source. The information must suffice to ensure that the continued functioning of the modified object code is in no case prevented or interfered with solely because modification has been made.

If you convey an object code work under this section in, or with, or specifically for use in, a User Product, and the conveying occurs as part of a transaction in which the right of possession and use of the User Product is transferred to the recipient in perpetuity or for a fixed term (regardless of how the transaction is characterized), the Corresponding Source conveyed under this section must be accompanied by the Installation Information. But this requirement does not apply if neither you nor any third party retains the ability to install modified object code on the User Product (for example, the work has been installed in ROM).

The requirement to provide Installation Information does not include a requirement to continue to provide support service, warranty, or updates for a work that has been modified or installed by the recipient, or for the User Product in which it has been modified or installed. Access to a network may be denied when the modification itself materially and adversely affects the operation of the network or violates the rules and protocols for communication across the network.

Corresponding Source conveyed, and Installation Information provided, in accord with this section must be in a format that is publicly documented (and with an implementation available to the public in source code form), and must require no special password or key for unpacking,

systems

reading or copying.

7. Additional Terms.

"Additional permissions" are terms that supplement the terms of this License by making exceptions from one or more of its conditions. Additional permissions that are applicable to the entire Program shall be treated as though they were included in this License, to the extent that they are valid under applicable law. If additional permissions apply only to part of the Program, that part may be used separately under those permissions, but the entire Program remains governed by this License without regard to the additional permissions.

When you convey a copy of a covered work, you may at your option remove any additional permissions from that copy, or from any part of it. (Additional permissions may be written to require their own removal in certain cases when you modify the work.) You may place additional permissions on material, added by you to a covered work, for which you have or can give appropriate copyright permission.

Notwithstanding any other provision of this License, for material you add to a covered work, you may (if authorized by the copyright holders of that material) supplement the terms of this License with terms:

a) Disclaiming warranty or limiting liability differently from the terms of sections 15 and 16 of this License; or b) Requiring preservation of specified reasonable legal notices or author attributions in that material or in the Appropriate Legal Notices displayed by works containing it; or c) Prohibiting misrepresentation of the origin of that material, or requiring that modified versions of such material be marked in reasonable ways as different from the original version; or d) Limiting the use for publicity purposes of names of licensors or authors of the material; or e) Declining to grant rights under trademark law for use of some trade names, trademarks, or service marks; or f) Requiring indemnification of licensors and authors of that material by anyone who conveys the material (or modified versions of it) with contractual assumptions of liability to the recipient, for any liability that these contractual assumptions directly impose on those licensors and authors.

All other non-permissive additional terms are considered "further restrictions" within the meaning of section 10. If the Program as you received it, or any part of it, contains a notice stating that it is governed by this License along with a term that is a further restriction, you may remove that term. If a license document contains a further restriction but permits relicensing or conveying under this License, you may add to a covered work material governed by the terms of that license document, provided that the further restriction does not survive such relicensing or conveying.

If you add terms to a covered work in accord with this section, you must place, in the relevant source files, a statement of the additional terms that apply to those files, or a notice indicating where to find the applicable terms.

Additional terms, permissive or non-permissive, may be stated in the form of a separately written license, or stated as exceptions; the above requirements apply either way.

8. Termination.

You may not propagate or modify a covered work except as expressly provided under this License. Any attempt otherwise to propagate or modify it is void, and will automatically terminate your rights under this License (including any patent licenses granted under the third paragraph of section 11).

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright holder, and you cure the violation prior to 30 days after your receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, you do not qualify to receive new licenses for the same material under section 10.

9. Acceptance Not Required for Having Copies.

You are not required to accept this License in order to receive or run a copy of the Program. Ancillary propagation of a covered work occurring solely as a consequence of using peer-to-peer transmission to receive a copy likewise does not require acceptance. However, nothing other than this License grants you permission to propagate or modify any covered work. These actions infringe copyright if you do not accept this License. Therefore, by modifying or propagating a covered work, you indicate your acceptance of this License to do so.

10. Automatic Licensing of Downstream Recipients.

Each time you convey a covered work, the recipient automatically receives a license from the original licensors, to run, modify and propagate that work, subject to this License. You are not responsible for enforcing compliance by third parties with this License.

An "entity transaction" is a transaction transferring control of an organization, or substantially all assets of one, or subdividing an organization, or merging organizations. If propagation of a covered work results from an entity transaction, each party to that transaction who receives a copy of the work also receives whatever licenses to the work the party's predecessor in interest had or could give under the previous paragraph, plus a right to possession of the Corresponding Source of the work from the predecessor in interest, if the predecessor has it or can get it with reasonable efforts.

You may not impose any further restrictions on the exercise of the rights granted or affirmed under this License. For example, you may not impose a license fee, royalty, or other charge for exercise of rights granted under this License, and you may not initiate litigation (including a cross-claim or counterclaim in a lawsuit) alleging that any patent claim is infringed by making, using, selling, offering for sale, or importing the Program or any portion of it.

11. Patents.

A "contributor" is a copyright holder who authorizes use under this License of the Program or a work on which the Program is based. The work thus licensed is called the contributor's "contributor version".

A contributor's "essential patent claims" are all patent claims owned or controlled by the contributor, whether already acquired or hereafter acquired, that would be infringed by some manner, permitted by this License, of making, using, or selling its contributor version, but do

not include claims that would be infringed only as a consequence of further modification of the contributor version. For purposes of this definition, "control" includes the right to grant patent sublicenses in a manner consistent with the requirements of this License.

ELTEC

systems

Each contributor grants you a non-exclusive, worldwide, royalty-free patent license under the contributor's essential patent claims, to make, use, sell, offer for sale, import and otherwise run, modify and propagate the contents of its contributor version.

In the following three paragraphs, a "patent license" is any express agreement or commitment, however denominated, not to enforce a patent (such as an express permission to practice a patent or covenant not to sue for patent infringement). To "grant" such a patent license to a party means to make such an agreement or commitment not to enforce a patent against the party.

If you convey a covered work, knowingly relying on a patent license, and the Corresponding Source of the work is not available for anyone to copy, free of charge and under the terms of this License, through a publicly available network server or other readily accessible means, then you must either (1) cause the Corresponding Source to be so available, or (2) arrange to deprive yourself of the benefit of the patent license for this particular work, or (3) arrange, in a manner consistent with the requirements of this License, to extend the patent license to downstream recipients. "Knowingly relying" means you have actual knowledge that, but for the patent license, your conveying the covered work in a country, or your recipient's use of the covered work in a country, would infringe one or more identifiable patents in that country that you have reason to believe are valid.

If, pursuant to or in connection with a single transaction or arrangement, you convey, or propagate by procuring conveyance of, a covered work, and grant a patent license to some of the parties receiving the covered work authorizing them to use, propagate, modify or convey a specific copy of the covered work, then the patent license you grant is automatically extended to all recipients of the covered work and works based on it.

A patent license is "discriminatory" if it does not include within the scope of its coverage, prohibits the exercise of, or is conditioned on the non-exercise of one or more of the rights that are specifically granted under this License. You may not convey a covered work if you are a party to an arrangement with a third party that is in the business of distributing software, under which you make payment to the third party based on the extent of your activity of conveying the work, and under which the third party grants, to any of the parties who would receive the covered work from you, a discriminatory patent license (a) in connection with copies of the covered work conveyed by you (or copies made from those copies), or (b) primarily for and in connection with specific products or compilations that contain the covered work, unless you entered into that arrangement, or that patent license was granted, prior to 28 March 2007.

Nothing in this License shall be construed as excluding or limiting any implied license or other defenses to infringement that may otherwise be available to you under applicable patent law.

12. No Surrender of Others' Freedom.

If conditions are imposed on you

(whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot convey a covered work so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not convey it at

all. For example, if you agree to terms that obligate you to collect a royalty for further conveying from those to whom you convey the Program, the only way you could satisfy both those terms and this License would be to refrain entirely from conveying the Program.

ELTEC

systems

13. Use with the GNU Affero General Public License.

Notwithstanding any other provision of this License, you have permission to link or combine any covered work with a work licensed under version 3 of the GNU Affero General Public License into a single combined work, and to convey the resulting work. The terms of this License will continue to apply to the part which is the covered work, but the special requirements of the GNU Affero General Public License, section 13, concerning interaction through a network will apply to the combination as such.

14. Revised Versions of this License.

The Free Software Foundation may publish revised and/or new versions of the GNU General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies that a certain numbered version of the GNU General Public License "or any later version" applies to it, you have the option of following the terms and conditions either of that numbered version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of the GNU General Public License, you may choose any version ever published by the Free Software Foundation.

If the Program specifies that a proxy can decide which future versions of the GNU General Public License can be used, that proxy's public statement of acceptance of a version permanently authorizes you to choose that version for the Program.

Later license versions may give you additional or different permissions. However, no additional obligations are imposed on any author or copyright holder as a result of your choosing to follow a later version.

15. Disclaimer of Warranty.

THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. Limitation of Liability.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MODIFIES AND/OR CONVEYS THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

17. Interpretation of Sections 15 and 16.

If the disclaimer of warranty

and limitation of liability provided above cannot be given local legal effect according to their terms, reviewing courts shall apply local law that most closely approximates an absolute waiver of all civil liability in connection with the Program, unless a warranty or assumption of liability accompanies a copy of the Program in return for a fee.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively state the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

This program is free software: you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation, either version 3 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program. If not, see https://www.gnu.org/licenses/.

Also add information on how to contact you by electronic and paper mail.

If the program does terminal interaction, make it output a short notice like this when it starts in an interactive mode:

<program> Copyright (C) <year> <name of author> This program comes with ABSOLUTELY NO WARRANTY; for details type \`show w'. This is free software, and you are welcome to redistribute it under certain conditions; type \`show c' for details.

The hypothetical commands \`show w' and \`show c' should show the appropriate parts of the General Public License. Of course, your program's commands might be different; for a GUI interface, you would use an "about box".

You should also get your employer (if you work as a programmer) or school, if any, to sign a "copyright disclaimer" for the program, if necessary. For more information on this, and how to apply and follow the GNU GPL, see https://www.gnu.org/licenses/.

The GNU General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Lesser General Public License instead of this License. But first, please read <https://www.gnu.org/licenses/why-not-lgpl.html>.

Copyright notice see above.

This license document may be reproduced and distributed unchanged, but no modifications are permitted. Translation: <www-en>, 2011-2014, 2016.

13 APPENDIX: SNMP OID OVERVIEW

This overview is also available with factory settings via the web interface using the URL: http://192.168.100.1/snmpd.txt.

SNMP command overview for the CyBox AP family (automatically generated) # # # SNMPSET commands: # # radio0_up # radio0_down # radio1_up # radio1_down # modem0_up # modem1_up # modem2_up # modem3_up # modem4_up # modem0_down # modem1_down # modem2_down # modem3_down # modem4_down # modem0_simslot <value> # modem1_simslot <value> # modem2_simslot <value> # modem3_simslot <value> # modem4_simslot <value> # network<index>.<entry> <value> # radio<index>.<entry> <value>

```
# wireless<index>.<entry> <value>
# uci <command> <config>.<section>[.<option>]=<value>
# service <name> <action>
# reboot
#
# SNMPSET system call:
#
# snmpset -c private -v 2c <IPv4> 1.3.6.1.4.1.2021.8.1 s <command string
or set entry string>
#
#
#
# SNMPGET/SNMPWALK objects:
#
# see list below
#
# SNMPGET system call:
#
# snmpget -c public -v 2c <IPv4> 1.3.6.1.4.1.2021.8.1.2.<ID>.101.1
#
# SNMPWALK system call:
#
# snmpwalk -c public -v 2c <IPv4> 1.3.6.1.4.1.2021.8.1.2.<ID>
#
##### system Table0 objects #####
boardname 1.3.6.1.4.1.2021.8.1.2.100
serial_number 1.3.6.1.4.1.2021.8.1.2.101
uboot_version 1.3.6.1.4.1.2021.8.1.2.102
firmware_version 1.3.6.1.4.1.2021.8.1.2.103
config_version 1.3.6.1.4.1.2021.8.1.2.104
uptime 1.3.6.1.4.1.2021.8.1.2.105
loadavg 1.3.6.1.4.1.2021.8.1.2.106
temperature 1.3.6.1.4.1.2021.8.1.2.107
uci_get 1.3.6.1.4.1.2021.8.1.2.108
```

customl 1.3.6.1.4.1.2021.8.1.2.109 custom2 1.3.6.1.4.1.2021.8.1.2.110 custom3 1.3.6.1.4.1.2021.8.1.2.111 mpstat 1.3.6.1.4.1.2021.8.1.2.112 ###### system Table0 objects ##### network_order 1.3.6.1.4.1.2021.8.1.2.150 ----listing not printed here, see console command on top of this page for live listing. The editor.----

14 APPENDIX: DEFAULT FACTORY SETTINGS

When shipped, the device has the following default settings:

Defaults for Ethernet 1 (all models):

Interface	IPV4 address type	Address	Remark
lan	static IPv4 address	192.168.100.1/24	
lan_alias	static IPv4 address	Calculated based on serial number	See chapter 4.1 IP Addresses of the CyBox AP 3
lan_dhcp	IPv4 DHCP client		
lan_mac	static IPv4 address	Calculated based on eth0 MAC address	See chapter 4.1 IP Addresses of the CyBox AP 3

Defaults for Ethernet 2:

Interface	IPV4 address	Address	Remark
wan	IPv4 DHCP client		
wan6	IPv6 DHCP client		

Other Defaults (all models):

Interface	Parameter	Remark
Password for user 'root'	root	Be sure to change it before deployment
WLAN, LTE, GPS	disabled	
Bridge	disabled	
DHCP/DNS server	disabled	
Firewall	<i>'Input'</i> and <i>'Output'</i> are set to <i>ACCEPT</i> , <i>'Forward'</i> is set to <i>REJECT</i>	

VLAN

Not configured

Network
LAN_ALIAS
eth0

LAN_DHCP
<u></u>
eth0

LAN	
eth0	
eth0	

WAN	
eth1	
eth1	
WAN6	

.

eth1

IPv4: 192.168.100.1/24 IPv6: fdff:a58d:4d24::1/60 Uptime: 0h 0m 0s MAC-Address: 00:00:5B: RX: 0 B (0 Pkts.) TX: 0 B (0 Pkts.)

Uptime: 0h 0m 0s MAC-Address: 00:00:5B: RX: 0 B (0 Pkts.) TX: 0 B (0 Pkts.)

Default Network Configuration

Status

Uptime: 0h 0m 60s MAC-Address: 00:00:5B: RX: 34.58 KB (416 Pkts.) TX: 149.14 KB (297 Pkts.) IPv4: 10.7.138.70/8 Uptime: 0h 0m 0s MAC-Address: 00:00:5B: RX: 34.58 KB (416 Pkts.) TX: 149.14 KB (297 Pkts.) Uptime: 0h 0m 60s MAC-Address: 00:00:5B: RX: 34.58 KB (416 Pkts.) TX: 149.14 KB (297 Pkts.) IPv4: 10.3.180.190/8 Uptime: 0h 0m 60s MAC-Address: 00:00:5B: RX: 34.58 KB (416 Pkts.) TX: 149.14 KB (297 Pkts.)