ELTEC systems

CYBOX AP 2

WIRELESS ACCESS POINT

KONFIGURATIONSHANDBUCH

Version: 1.0 für Firmware V20.36.03 | Datum: 14.04.2021

Inhalt

1 WICHTIGE INFORMATIONEN

1.1 Revision

Interne Version: ff6db28

Revision	Änderungen	Datum
1.0	Erste Version für diese Firmware	14.04.2021

1.2 Disclaimer

1.2.1 Urheberrechtshinweis

1.2.2 GPL-Erklärung für CyBox-Software

Dieses Softwareprodukt enthält Software, die von der GNU-GPL abgedeckt wird (siehe unten in diesem Dokument). Es kann auch andere Teile enthalten, die von anderen Lizenzen abgedeckt werden (z. B. LGPL). Eine Liste aller Module und ihrer Lizenzen („FOSS“-Liste) ist auf Anfrage erhältlich (siehe Link unten). Der Quellcode aller GPL-abgedeckten Module kann auch von den Besitzern der CyBox AP 2-W/LTE angefordert werden (siehe Link unten).

Für die GPL-abgedeckten Teile gilt diese Lizenz:

```
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 und Quellen sind aus Platzgründen nicht in der Binärdistribution in den Produkten und in der Produktdokumentation enthalten.

Verwenden Sie diesen Link, um FOSS und Quellen anzufordern. Bitte senden Sie Ihre Anfrage per Post (möglicherweise fallen Bearbeitungsgebühren für Quellen an):

ELTEC Elektronik AG

Galileo-Galilei-Str. 11

55129 Mainz

Germany

1.2.2.1 Gewährleistungsausschluß

ES BESTEHT KEINERLEI GEWÄHRLEISTUNG FÜR DAS PROGRAMM, SOWEIT DIES GESETZLICH ZULÄSSIG IST. SOFERN NICHT ANDERWEITIG SCHRIFTLICH BESTÄTIGT, STELLEN DIE URHEBERRECHTSINHABER UND/ODER DRITTE DAS PROGRAMM SO ZUR VERFÜGUNG, „WIE ES IST“, OHNE IRGENDEINE GEWÄHRLEISTUNG, WEDER AUSDRÜCKLICH NOCH IMPLIZIT, EINSCHLIEßLICH – ABER NICHT BEGRENZT AUF – DIE IMPLIZITE GEWÄHRLEISTUNG DER MARKTREIFE ODER DER VERWENDBARKEIT FÜR EINEN BESTIMMTEN ZWECK. DAS VOLLE RISIKO BEZÜGLICH QUALITÄT UND LEISTUNGSFÄHIGKEIT DES PROGRAMMS LIEGT BEI IHNEN. SOLLTE SICH DAS PROGRAMM ALS FEHLERHAFT HERAUSSTELLEN, LIEGEN DIE KOSTEN FÜR NOTWENDIGEN SERVICE, REPARATUR ODER KORREKTUR BEI IHNEN.

1.2.2.2 Haftungsbegrenzung

IN KEINEM FALL, AUßER WENN DURCH GELTENDES RECHT GEFORDERT ODER SCHRIFTLICH ZUGESICHERT, IST IRGENDEIN URHEBERRECHTSINHABER ODER IRGENDEIN DRITTER, DER DAS PROGRAMM WIE OBEN ERLAUBT MODIFIZIERT ODER ÜBERTRAGEN HAT, IHNEN GEGENÜBER FÜR IRGENDWELCHE SCHÄDEN HAFTBAR, EINSCHLIEßLICH JEGLICHER ALLGEMEINER ODER SPEZIELLER SCHÄDEN, SCHÄDEN DURCH SEITENEFFEKTE (NEBENWIRKUNGEN) ODER FOLGESCHÄDEN, DIE AUS DER BENUTZUNG DES PROGRAMMS ODER DER UNBENUTZBARKEIT DES PROGRAMMS FOLGEN (EINSCHLIEßLICH – ABER NICHT BESCHRÄNKT AUF – DATENVERLUSTE, FEHLERHAFTE VERARBEITUNG VON DATEN, VERLUSTE, DIE VON IHNEN ODER ANDEREN GETRAGEN WERDEN MÜSSEN, ODER DEM UNVERMÖGEN DES PROGRAMMS, MIT IRGENDEINEM ANDEREN PROGRAMM ZUSAMMENZUARBEITEN), SELBST WENN EIN URHEBERRECHTSINHABER ODER DRITTER ÜBER DIE MÖGLICHKEIT SOLCHER SCHÄDEN UNTERRICHTET WORDEN WAR.

Den folgenden Text sollten Sie in einer „About“-Box (siehe Registerkarte „System“) zusammen mit dem Produkt erhalten haben. Hier wird er als Referenz wiederholt:

```
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.de>. 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 Regulatorische Beschränkungen für Änderungen der Länder- und Sendeleistungseinstellungen

Stellen Sie sicher, dass nur Personen mit entsprechenden Kenntnissen, auch in regulatorischen Belangen, Zugriff auf die Konfigurationseinstellungen des Access Points haben. Sie müssen sich der Konsequenzen einer unsachgemäßen Einstellung von Land und Sendeleistung bewusst sein (möglicherweise gibt es zusätzliche Einstellungen). Dazu muss das Standard-Konfigurationspasswort geändert werden, bevor der Access Point

eingesetzt wird. Dieses neue Passwort darf nur an sachkundige und verantwortliche Personen weitergegeben werden.

Ein Beispiel für eine Regelung, die sich auf die Länderauswahl auswirkt, ist, dass in Deutschland ab Oktober 2016 die Frequenzen im Bereich 5150 MHz - 5350 MHz nur noch in geschlossenen Räumen und ähnlichen Umgebungen verwendet werden dürfen. Für weitere Informationen siehe www.bundesnetzagentur.de.

1.3 Bekannte Fehler

- Beim Betrieb von WLAN im 11ac-Modus wird die Datenübertragungsrate fälschlicherweise mit 6 Mbit/s angegeben.

2 ÜBER DIESES DOKUMENT

Dieses Konfigurationshandbuch richtet sich an Systementwickler und Integratoren. Es ist nicht für Endbenutzer gedacht. Es beschreibt die Firmware-Funktionen der Access Point/Router/Gateway-Produktfamilie und liefert Informationen für spezielle Anwendungen und Konfigurationen des Produkts.

Dieses Handbuch soll Sie durch den Konfigurationsprozess eines Access Points/Routers/Gateways (die Namen werden in diesem Handbuch synonym verwendet) für den Einsatz in einem Zug oder Bus führen. Wir haben versucht, die Hauptaspekte dieser Aufgabe abzudecken, einschließlich

- Sicherung und Wiederherstellung von Konfigurationen
- Installieren neuer Firmware-Versionen
- Handhabung von IP-Adressen, DHCP, VLAN, VPN, Firewall
- Konfiguration von WiFi und LTE
- MWAN-Konfiguration für mehrere WAN-Verbindungen
- ELTECs Zugkopplung und Wireless-Backbone-Protokoll ICCP
- Fernverwaltung über SNMP
- Skripting und UCI.

Nicht enthalten ist eine vollständige Auflistung aller Funktionen und aller Konfigurationselemente im Detail.

Informationen zur mechanischen und elektrischen Installation der Access Points finden Sie in einem separaten produktspezifischen Installationshandbuch, das Sie im Download Center unter www.eltec.de herunterladen können.

2.1 Hinweise zu Formatierungen

In den folgenden Abschnitten bezieht sich der mit `diesem Stil` formatierte Text auf Titel, Registerkarten, Felder, Menünamen, Gruppennamen, Tasten und andere beschreibendene Texte auf der webbasierten Konfigurations-Benutzeroberfläche („LuCI“). Sie werden durch „→“ gruppiert.

Dieses Markup wird für alle Navigationselemente verwendet, die für den Zugriff auf Einstellungen benötigt werden, unabhängig von den Elementen, die zum Anklicken verwendet werden, oder nur zur visuellen Gruppierung.

Für eingetippten Text wird eine `Schreibmaschinenschrift` verwendet.

3 ÜBER DIE CyBox AP 2

Die CyBox AP 2 ist ein Mitglied unserer CyBox-Familie von robusten Wireless Railway Access Points. Sie ist speziell für die Anforderungen von Schienenfahrzeug-Applikationen konzipiert und bietet stabile, sichere und breitbandige Verbindungen zwischen dem lokalen Ethernet und Wireless-Clients. Mit Hilfe des Access Points haben mehrere mobile Wi-Fi-fähige Geräte in einem Personenzug oder einer U-Bahn die Möglichkeit, beispielsweise mit dem Internet zu kommunizieren oder auf lokale Daten zuzugreifen.

Die CyBox AP 2 Firmware bietet eine komfortable Management-Schnittstelle über einen Webdienst. Die Open-Source-Software ermöglicht neben der Einstellung globaler Setup-Parameter auch die Konfiguration der Funkschnittstellen wie Kanalauswahl, SSID, Verschlüsselungsschlüssel und Firewall-Setup. Die Access Point- und Router-Konfigurationen sowie die Management-Firmware können remote aktualisiert werden.

Die Firmware des Geräts basiert auf Linux und OpenWRT/LEDE. Open Source-Informationen finden Sie im Vorwort.

4 ZUGRIFF AUF DIE CyBox AP 2

Die CyBox AP 2 kann auf verschiedene Arten konfiguriert werden:

1. Die grafische Web-Oberfläche
2. Die Kommandozeilenschnittstelle über eine SSH- oder serielle Verbindung (siehe Kapitel 10 SSH / SERIELLE KONSOLE)
3. Mit einem USB-Stick (um die Firmware zu aktualisieren oder eine vorbereitete Konfiguration anzuwenden, siehe Kapitel 11.2 USB-Möglichkeiten)
4. Mit SNMP (siehe Kapitel 7 SNMP)

4.1 IP-Adressen der CyBox AP 2

Standardmäßig ist die CyBox AP 2 über die folgenden IP-Adressen erreichbar (siehe Abbildung Die Seite Network → Interfaces (Standardeinstellungen)):

- 192.168.100.1 (LAN)
- Eine über DHCP bezogene Adresse (wenn möglich LAN_DHCP)
- Eine aus der Seriennummer abgeleitete Adresse (LAN_ALIAS)
- Eine von der MAC des ersten Ethernet-Ports abgeleitete Adresse (LAN_MAC)

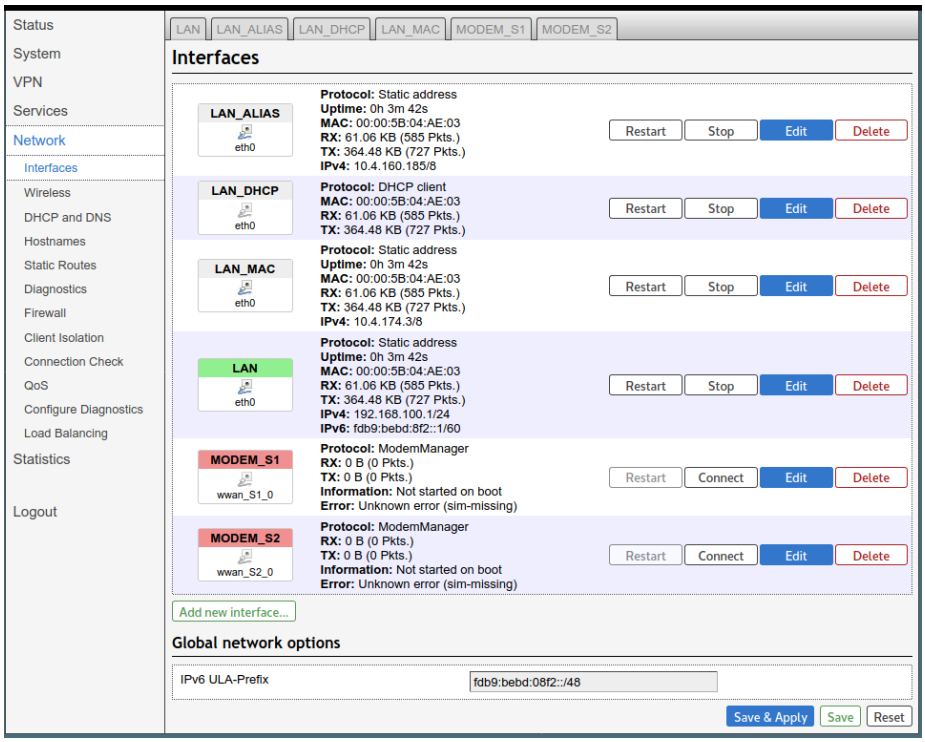
Die LAN_ALIAS-Adresse wird wie folgt aus der Seriennummer (die auf dem Typenschild aufgedruckt ist) abgeleitet (Beispiel Seriennummer: EL303289):

1. Nicht-Ziffern entfernen: `303289`
2. Als sechsstelliger Hex-Wert drucken: `0x04A0B9`
3. Verwenden Sie die oberen 8 Bits für x, die mittleren für y und die unteren für z: `x=0x04 y=0xA0 z=0xB9`
4. Wandeln Sie x,y,z in Dezimalzahlen um: `x=4 y=160 z=185`
5. Die LAN_ALIAS-Adresse lautet `10.4.160.185`

In ähnlicher Weise ergibt sich die LAN_MAC-Adresse aus der MAC-Adresse der ersten Ethernet-Schnittstelle, die auf dem Typenschild aufgedruckt ist (Beispiel MAC `00:00:5B:04:AE:03`):

1. Nehmen Sie die letzten drei Bytes: `04:AE:03`
2. Verwenden Sie die oberen 8 Bits für x, die mittleren für y und die unteren für z : `x=0x04 y=0xAE z=0x03`
3. Wandeln Sie x,y,z in Dezimalzahlen um: `x=4 y=174 z=3`
4. Die LAN_MAC-Adresse lautet `10.4.174.4`

Sie können nicht benötigte Netzwerkschnittstellen löschen, indem Sie in der Weboberfläche auf die rote Schaltfläche „Löschen“ klicken.



Die Seite Network → Interfaces (Standardeinstellungen)

4.2 Zugang zum Web-Interface

Vor dem Zugriff auf das Web-Interface muss Ihr Computer mit dem Ethernet-Port LAN 1 verbunden und so konfiguriert sein, dass er dasselbe Subnetz wie die CyBox AP 2 verwendet.

Auf die Weboberfläche kann über HTTPS unter den folgenden IP-Adressen zugegriffen werden: 4.1 IP-Adressen der CyBox AP 2 (Standard: https://192.168.100.1/ im Subnetz `192.168.100.0/24`). Es wird ein selbstsigniertes SSL-Zertifikat verwendet. Ihr Browser sollte Sie davor warnen. Sie können entweder das Zertifikat akzeptieren oder auf HTTP zurückgreifen: http://192.168.100.1/.

Verwenden Sie auf der Login-Seite den Benutzernamen `root` und das Passwort `root`. Natürlich sollten Sie das Passwort 5.1 Ändern des Passwortes .

Sobald die Verbindung hergestellt ist, können Sie durch die verschiedenen Registerkarten navigieren, um mit der Konfiguration zu beginnen. Es gelten einige Regeln:

- Um Ihre Konfiguration anzuwenden und auch zu speichern, klicken Sie auf die Schaltfläche `Save & Apply` in der unteren rechten Ecke der meisten Seiten. Wenn Sie nicht auf diese Schaltfläche klicken, werden Ihre Änderungen verworfen.
- Gespeicherte Konfigurationen bleiben auch nach einem Neustart erhalten.
- Wenn IP-Adressen geändert werden, muss der Access Point unter der neuen URL im Browser angesprochen werden.

5 QUICK START QUIDE

Dieses Kapitel beschreibt die Schritte zur Konfiguration des Standard-Access-Points. Das Gerät muss elektrisch angeschlossen sein (siehe Installationshandbuch). Die werkseitigen Standardeinstellungen werden verwendet.

Dieses Kapitel zeigt einige gängige Anwendungsfälle und jeweils eine beispielhafte Implementierung.

Wenn die Konfiguration der CyBox AP 2 tiefgreifende Änderungen erfordert, z.B. für einen neuen Anwendungsfall, besteht die Gefahr, dass frühere (möglicherweise inzwischen vergessene) Einstellungen mit der neuen Konfiguration in Konflikt geraten. Daher wird empfohlen, die Konfiguration mit den werkseitigen Standardeinstellungen zu starten. Wenn Sie den Hardware-Reset-Schalter länger als 5 Sekunden drücken, werden die Werkseinstellungen wiederhergestellt.

Das Webinterface bietet die gleiche Funktion: `System` → `Backup / Flash Firmware` → `Perform reset`.

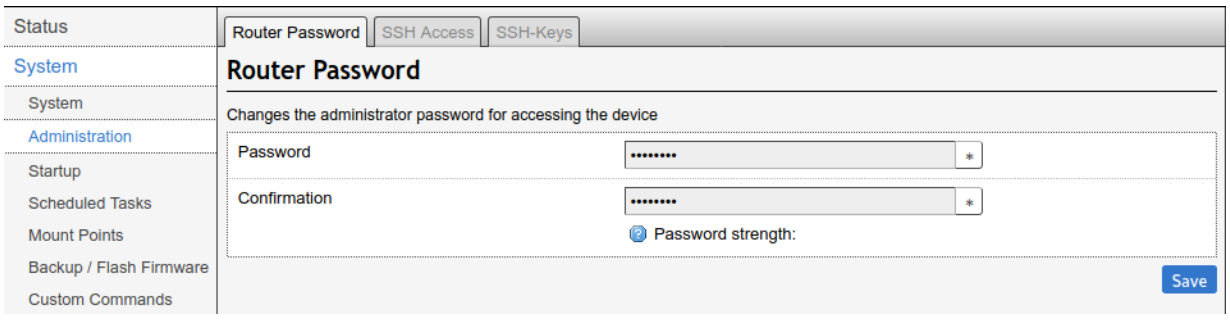
Für alle nachfolgenden Konfigurationsbeispiele wird folgende Ausgangssituation angenommen:

- Die CyBox AP 2 ist in Betrieb
- Die CyBox AP 2 wurde auf Werkseinstellungen zurückgesetzt. Die IP-Adresse lautet 192.168.100.1
- Standard-Passwort des Root-Benutzers: „root“
- Bediener-Arbeitsplatz und CyBox AP 2 sind über Ethernet verbunden
- Der Arbeitsplatz-Browser ist an der CyBox AP 2-Weboberfläche angemeldet
- Der Bediener ist zusätzlich über SSH an der CyBox AP 2 angemeldet (falls vorhanden, wäre ein serielles Konsolenterminal vorzuziehen).

In den folgenden Beispielen werden [eckige Klammern] verwendet, um Aktionen zu kennzeichnen, die keine Interaktion des Bedieners erfordern, weil sie automatisch ablaufen oder bereits ausgeführt wurden (die Erwähnung hier kann hilfreich sein, um zu überprüfen, ob die Konfiguration richtig ist).

5.1 Ändern des Passwortes

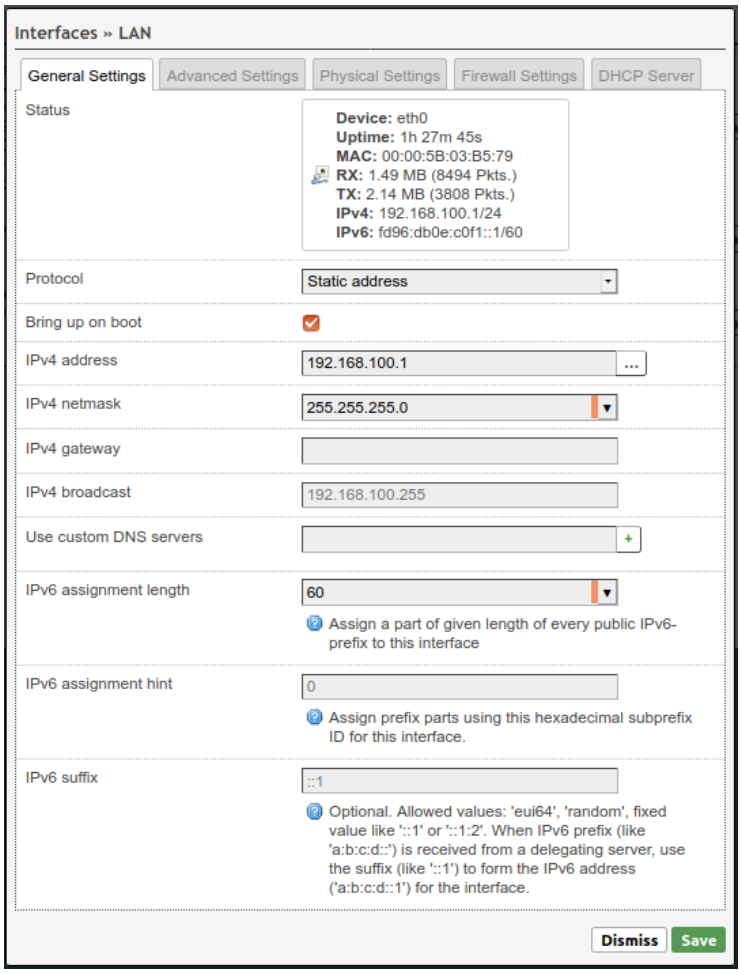
Das Passwort sollte zuerst geändert werden, um rechtliche Konsequenzen zu vermeiden, wie im Vorwort beschrieben. Der Standard-Benutzer/das Standard-Passwort ist ‘root’/’root’. Um es zu ändern, gehen Sie zu `System` → `Administration`, geben Sie ein neues Passwort ein und klicken Sie auf `Save`.



Ändern des Passworts

5.2 LAN-IP-Adresse ändern (Kurzanleitung)

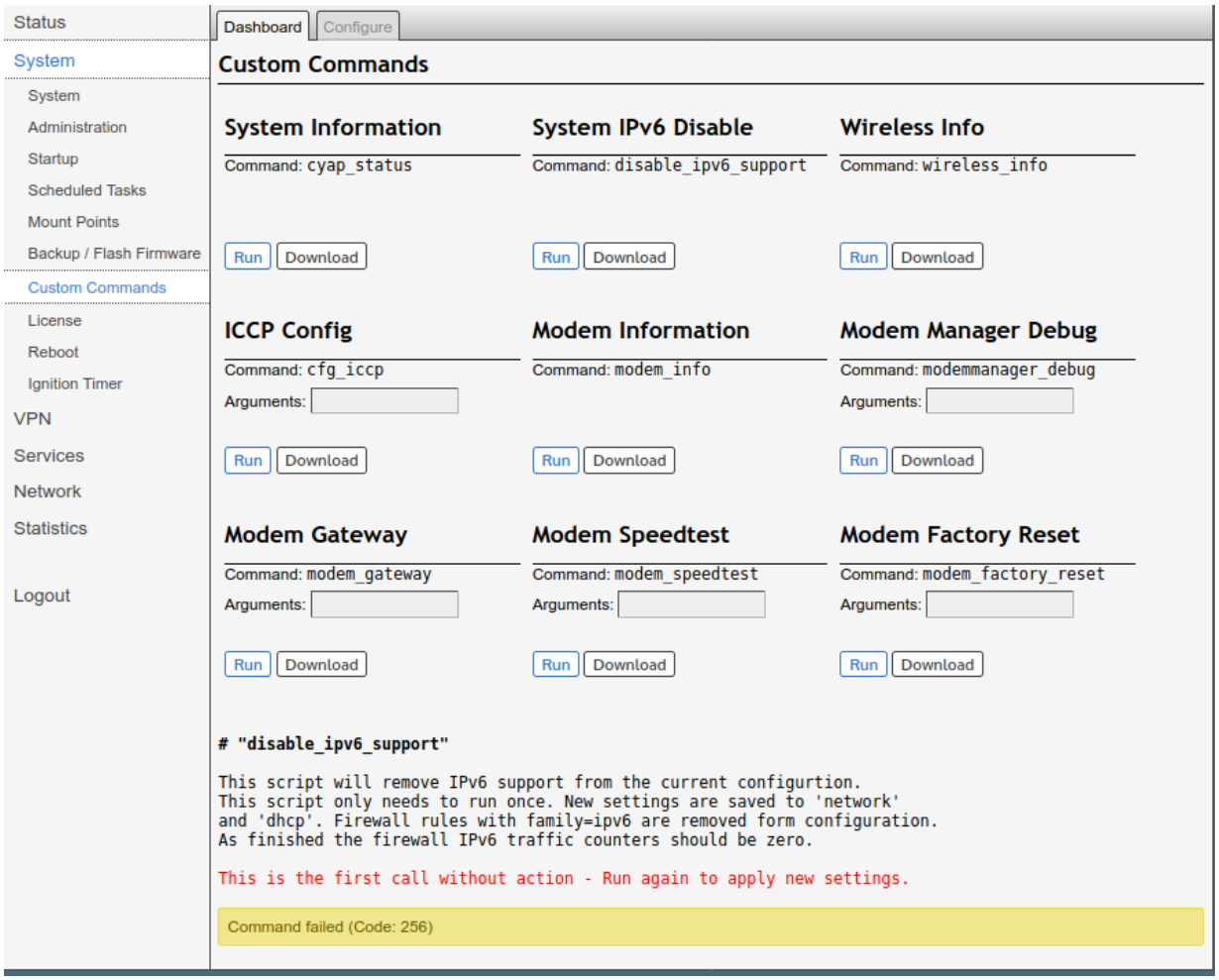
Die werkseitig voreingestellte IP-Adresse 192.168.100.1 muss geändert werden, um Ihrer Netzwerktopologie zu entsprechen. Öffnen Sie `Network` → `Interfaces` und klicken Sie auf die Schaltfläche `Edit` des Interfaces LAN. Ändern Sie die IP-Adresse (Feld `IPv4 address`) oder ändern Sie das Feld `Protocol` in `DHCP-Client` und klicken Sie dann auf `Save & Apply`. Um wieder auf die Weboberfläche zugreifen zu können, müssen Sie die neue IP-Adresse in Ihren Browser eingeben.



Beispiel für eine LAN-Konfiguration

5.2.1 Deaktivieren von IPv6

Das benutzerdefinierte Hilfsskript unter `System` → `Custom Commands` → `Dashboard` ändert die Netzwerk/Firewall-Konfiguration, um den gesamten IPv6-Netzwerkverkehr zu deaktivieren. Normalerweise haben alle Netzwerkschnittstellen eine automatisch zugewiesene IPv6-Adresse. Wenn in Ihrer Umgebung kein Bedarf für IPv6-Netzwerkverkehr besteht, sollten Sie dieses Skript in frühen Konfigurationsschritten verwenden, um alle IPv6-Adresseinstellungen von Netzwerkschnittstellen und IPv6-Firewall-Regeln zu entfernen. Beachten Sie, dass die Run-Schaltfläche zweimal ausgeführt werden muss. Das erste Mal dient nur der Benutzerinformation. Die Änderung der Konfiguration ist dauerhaft.



Deaktivieren der Netzwerk-IPv6-Unterstützung - erster Durchlauf

5.3 Beispiel: Localer Access Point

In einem ersten Schritt wird ein einfacher Access Point konfiguriert. Das kabelgebundene Ethernet und die drahtlosen Funkmodule bilden eine isolierte lokale Domäne, in der die CyBox AP 2 DHCP-Dienste bereitstellt. Abschließend zeigt das Beispiel unter „LAN IP-Adresse“, wie eine neue statische IP-Adresse eingestellt wird. Unter „Netzwerk > Schnittstellen → LAN → Protokoll“ können Sie das DHCP-Client-Setup so konfigurieren, dass eine IP-Adresse von einem DHCP-Server in Ihrem Netzwerk abgerufen wird. Der Access Point und seine Clients werden Teil einer weiteren lokalen Domäne, in der DHCP, DNS und ein Gateway bereitgestellt werden, wodurch die CyBox AP 2 und ihre Clients mit übergeordneten Netzwerken verbunden werden.

5.3.1 Systemeinstellungen

- Wählen Sie `System` → `System` (zwei verschachtelte *System*-Registerkarten).
- In der Box `System Properties` die `General Settings` auswählen und bei Bedarf die Einträge anpassen. Die Schaltfläche `Sync with browser` ist nützlich für Fälle, in denen kein NTP-Server verfügbar ist. Die Registerkarten `Logging` und `Language and Style` können vorerst ignoriert werden.
- Passen Sie bei Bedarf die Einträge in der Registerkarte `Time Synchronization` an.
- Klicken Sie auf die Schaltfläche `Save & Apply`

5.3.2 Vorbereiten des WLAN-Funk-Interfaces

- Wählen Sie `Network` → `Wireless`: Dies zeigt die Wireless-Controller *radio0* und *radio1* mit einigen Software-Tasten an.
- Wählen Sie die Registerkarte `radio0: Unknown "OpenWrt"` oder klicken Sie den `Edit`-Schalter des `radio0`
- In der Box *Device Configuration* (Gerätekonfiguration):
  - Wählen Sie die Registerkarte *Advanced Settings*
    - Wählen Sie im Dropdown-Menü *Country Code*, das Land des aktuellen Standorts aus
  - Wählen Sie die Registerkarte *General Setup*
    - Wählen Sie im Drop-Down-Menu *Mode* einen Modus aus, normalereise *N* oder *AC*
    - Wählen Sie im Drop-Down-Menu *Channel* einen Kanal (oder *auto*)
    - Wählen Sie bei Bedarf einen geeigneten Wert im Dropdown-Menü *Transmit Power*
- In der Box *Interface Configuration*:
  - [Wählen Sie die Registerkarte *General Setup*]
    - Geben Sie eine beliebige *ESSID* (wird unten als "WLssid" angegeben) ein
    - [*Mode*: Wählen Sie *Access Point*]
    - [Feld *Network*: Kontrollkästchen aktivieren *lan*]
    - [Feld *Network*: Kontrollkästchen deaktivieren *create*]
    - Aktivieren Sie bei Bedarf das Kontrollkästchen *Hide ESSID*
  - Wählen Sie die Registerkarte *Wireless Security*
    - Wählen Sie im Drop-Down-Menu *Encryption* nach Bedarf aus
    - Wählen Sie im Drop-Down-Menu *Cipher auto*, sofern kein bestimmter Algorithmus erforderlich ist
    - Geben Sie unter *Key* ein Passwort mit mindestens 8 Zeichen ein
- Klicken Sie auf die Schaltfläche *Save & Apply*
- Wählen Sie `Network` → `Wireless`
  - Klicken Sie für radio0 auf die Schaltfläche *Enable*

Zu diesem Zeitpunkt sollte die Funkschnittstelle für mögliche WLAN-Clients sichtbar werden und umgekehrt. Möglicherweise müssen Clients aufgefordert werden, nach verfügbaren Funknetzwerken zu suchen. Diese Clients werden dann in der Registerkarte *Network*, Registerkarte *WiFi*, Feld *Associated Stations* angezeigt.

5.3.3 Verbinden von radio0 mit dem Netzwerk

- Wählen Sie die Registerkarte *Network* Registerkarte *Interfaces* Registerkarte *LAN*
- In der Box *Common Configuration*
  - Wählen Sie die Registerkarte *Physical Settings*:
    - *Bridge interfaces*: Kontrollkästchen aktivieren

- [*Enable STP*: Kontrollkästchen *Spanning Tree Protocol on this bridge* deaktivieren]
- [*Interface*: Kontrollkästchen *Ethernet Adapter: „eth0“* aktivieren]
- *Interface*: Kontrollkästchen *Wireless Network: Master* “<SSID>” aktivieren
- [*Interface*: Kontrollkästchen *Custom Interface* deaktivieren]

- In der Box *DHCP Server*
  - Wählen Sie die Registerkarte *General Setup*
    - Kontrollkästchen *Disable DHCP for this interface* deaktivieren
  - Nehmen Sie bei Bedarf weitere Änderungen in den Registerkarten *General Setup* und *Advanced Settings* vor
- Klicken Sie auf die Schaltfläche *Save & Apply*

Nun verbindet die CyBox AP 2 das Ethernet und alle WLAN-Clients in der lokalen Domain 192.186.100.0 und stellt einen lokalen DHCP-Dienst bereit. Es besteht jedoch noch kein Uplink zu einem Gateway.

5.3.4 Verbindung zum WAN herstellen

Es ist das Ziel, dass die CyBox AP 2 ihre Clients über Ethernet in ein übergeordnetes Netzwerk integriert. DHCP-, DNS- und Gateway-Dienste sollen in diesem Netz verfügbar sein.

- Wählen Sie die Registerkarte *Network* Registerkarte *Interfaces* Registerkarte *LAN*
- Im Abschnitt *Common Configuration*:
  - Wählen Sie im Drop-Down-Menu *Protocol DHCP Client*
  - Klicken Sie auf die Schaltfläche *Switch Protocol*
- Klicken Sie auf die Schaltfläche *Save & Apply*

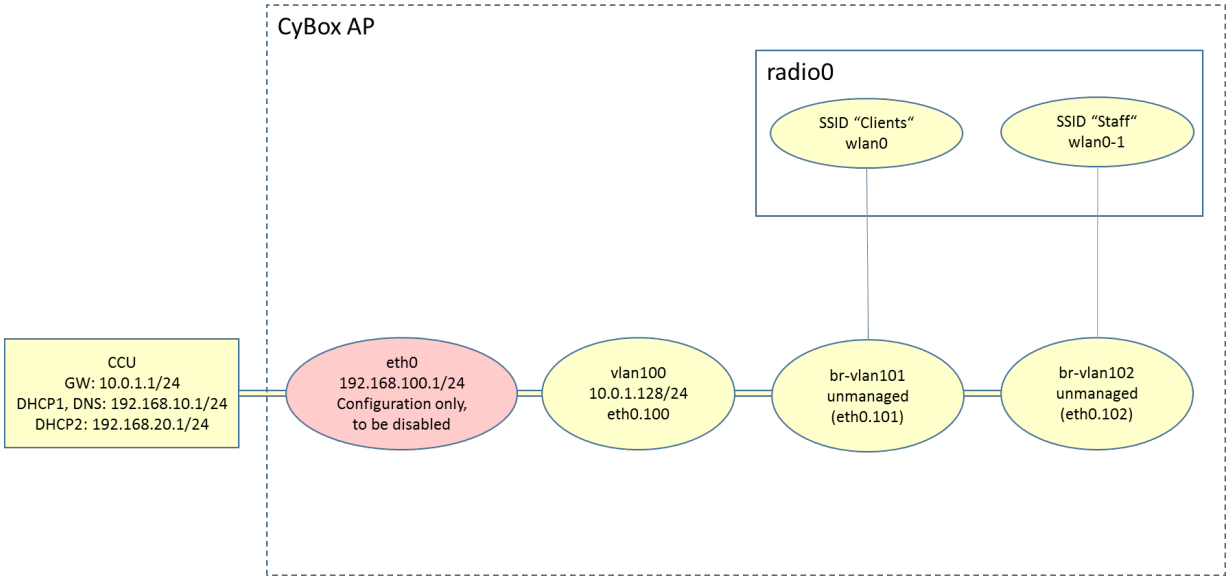
Damit wird die lokale Domain 192.186.100.0 beendet. Verbinden Sie nun die CyBox AP 2 über Ethernet mit der Gateway-Domäne, starten Sie die CyBox AP 2 neu (Hardware-Reset-Schalter verwenden) und verbinden Sie die WLAN-Clients erneut.

5.4 Beispiel: Verbinden von drei VLANs mit einem Server

In diesem Anwendungsfall bietet der Access Point 3 VLAN-Schnittstellen:

- eine für den Management-Zugriff über kabelgebundenes Ethernet, unter Verwendung einer statischen IP-Adresse
- ein unmanaged WLAN-Zugang für „Clients“, keine Verschlüsselung
- ein weiterer unmanaged WLAN-Zugang für „Staff“, verschlüsselt, optional versteckte SSID

Der Access Point ist über Ethernet mit einem Server (oder einem Host-Computer, in der folgenden Abbildung CCU genannt) verbunden, der DHCP-, DNS- und Gateway-Dienste bereitstellt. Nehmen Sie ausgehend von den Werkseinstellungen Systemeinstellungen vor, wie in Abschnitt 7.2.1 beschrieben (falls erforderlich).



Netzwerk-Topologie mit drei VLANs

5.4.1 Erstellen des Management-VLANs

Erstellen Sie eine neue Ethernet-Schnittstelle (eth0.100) und geben Sie ihr den Namen „vlan100“. Machen Sie sie zu einem vollwertigen Netzhost, indem Sie ihr eine statische Adresse und ein Gateway zuweisen.

- Wählen Sie die Registerkarte *Network* Registerkarte *Interfaces*
- Klicken Sie auf die Schaltfläche *Add new interface*
- Geben Sie bei *Name of new interface* folgendes ein: „vlan100”
- [Wählen Sie *Protocol of the new interface*: Static address]
- [Deaktivieren Sie das Kontrollkästchen „*Create a bridge over multiple interfaces*“]
- Geben Sie bei *Custom Interface* folgendes ein: “eth0.100”
- Klicken Sie auf die Schaltfläche *Submit*
- [Die Seite VLAN100 öffnet sich]
- [Registerkarte *Network* Registerkarte *Interfaces* Registerkarte *VLAN100* Registerkarte *General Setup*]
    - Geben Sie bei *IPv4 address* folgendes ein: “10.0.1.128”
    - Wählen Sie *IPv4 netmask* 255.255.255.0
    - Geben Sie bei *IPv4 gateway* folgendes ein: “10.0.1.1”
- Klicken Sie auf die Schaltfläche *Save & Apply*

5.4.2 Hinzufügen von zwei Unmanaged VLANs

Wir erstellen zwei weitere Ethernet-Schnittstellen eth0.101 und eth0.102 mit den Namen vlan101 bzw. vlan102.

- Netzwerk-Interfaces: Neues Interface hinzufügen → Name des neuen Interfaces: “vlan101”
- Protokoll der neuen Schnittstelle: Unmanaged
- [Deaktivieren Sie Create a bridge over multiple interfaces]
- Benutzerdefinierte Schnittstelle: “eth0.101 “

- Absenden
- [Seite VLAN101 öffnet sich]
- Klicken Sie auf die Schaltfläche *Save & Apply*

Machen Sie dasselbe für “vlan102” und “eth0.102”.

5.4.3 Konfigurieren und Aktivieren des/der Funkmodule(s)

Sie können frei wählen, welche Schnittstelle Sie welchem Funkmodul zuweisen möchten. Wenn beide Funkmodule verwendet werden sollen, muss dieser Abschnitt (7.3.3) auch für *radio1* ausgeführt werden.

- Wählen Sie die Registerkarte *Network* –> Registerkarte *WiFi* –> Registerkarte *radio0* (oder klicken Sie auf die Schaltfläche *Edit* auf *radio0*)
- In der Box *Device Configuration:*
    - Wählen Sie die Registerkarte *Advanced Settings*
        - Wählen Sie den Country Code
        - Wählen Sie den Modus

Die folgenden 3 Zeilen beheben ein Problem mit der LuCI-Seite (Das Dropdown- Menü für den Ländercode wird nicht korrekt aktualisiert)

- Klicken Sie auf die Schaltfläche *Save & Apply*
- Logout / Login
- Wählen Sie die Registerkarte *Network* –> Registerkarte *WiFi* –> Registerkarte *radio0* (oder klicken Sie auf die Schaltfläche *Edit* für *radio0*)

Jetzt können wir die Einstellungen für *radio0* vervollständigen:

- In der Box *Device Configuration*:
    - Wählen Sie die Registerkarte *Advanced Settings*
        - Wählen Sie *HT mode*
        - Wählen Sie *Channel*
        - Wählen Sie *Transmit Power*
- Klicken Sie auf die Schaltfläche *Save & Apply*
- Wählen Sie die Registerkarte *Network* –> Registerkarte *WiFi*
- Klicken Sie auf die Schaltfläche *Enable* für *radio0*

5.4.4 Verbinden von VLAN „Clients“ mit radio0

- Wählen Sie die Registerkarte *Network* –> Registerkarte *WiFi* –> Registerkarte *radio0* (oder klicken Sie auf die Schaltfläche *Edit* für *radio0*)
- In der Box *Interface Configuration*:
    - [Wählen Sie die Registerkarte *General Setup*]
        - Geben Sie bei *ESSID* folgendes ein: „Clients“
        - Deaktivieren Sie das Kontrollkästchen *lan*

- Aktivieren Sie das Kontrollkästchen *vlan101*

- Klicken Sie auf die Schaltfläche *Save & Apply*

5.4.5 Anschluss von VLAN „Staff“ an radio0

- Wählen Sie die Registerkarte *Network* Registerkarte *WiFi*
- Klicken Sie auf die Schaltfläche *Add* für *radio0* (wenn beide VLANs auf demselben Funkmodul laufen sollen).

Wenn „Staff“ das andere Funkmodul verwenden soll und dieses Funkmodul konfiguriert und aktiviert wurde (siehe 7.3.3), wählen Sie alternativ (anstelle von *Add*) die Registerkarte die Registerkarte *Network* Registerkarte *WiFi* Registerkarte *radio1* (oder klicken Sie auf die Schaltfläche *Edit* für *radio1*)

- In der Box *Interface Configuration*:
  - [Wählen Sie die Registerkarte *General Setup*]
    - Geben Sie bei *ESSID* folgendes ein: „Staff“
    - [Deaktivieren Sie das Kontrollkästchen *lan*]
    - Aktivieren Sie das Kontrollkästchen *vlan102*
    - Aktivieren Sie bei Bedarf das Kontrollkästchen *Hide ESSID*
  - Wählen Sie die Registerkarte *Wireless Security*
    - Wählen Sie *Encryption* (e.g. WPA2-PSK)
    - Geben Sie unter *Key* ein Passwort mit mindestens 8 Zeichen ein

- Klicken Sie auf die Schaltfläche *Save & Apply*

5.4.6 Überprüfen der Konfiguration

Zur Überprüfung können Sie sich über SSH an der CyBox AP 2 anmelden und den Befehl ifconfig aufrufen. Die folgenden Schnittstellen sollten angezeigt werden:

```
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 Deaktivierung der nicht benötigten Standardadresse

Nach erfolgreichem Test des VLAN-basierten Management-Zugangs (vlan100) kann die Standardadresse 192.168.100.1 deaktiviert werden. Dies wird durch Löschen der *LAN*-Schnittstelle erreicht:

- Wählen Sie die Registerkarte *Network* Registerkarte *Interface*
- Klicken Sie auf die Schaltfläche *Delete* für das *LAN*-Interface (normalerweise die unterste)
- Wählen Sie die Registerkarte *Network* Registerkarte *Interfaces* Registerkarte *LAN*

  Alternativ können Sie das Protokoll der *LAN* -Schnittstelle in *Unmanaged* ändern:
- Wählen Sie die Registerkarte *Network* Registerkarte *Interface* Registerkarte *LAN*
- In der Box *Common Configuration*:
  - Wählen Sie im Drop-Down-Menu *Protocol Unmanaged*
- Klicken Sie auf die Schaltfläche *Save & Apply*

5.5 Beispiel: Client Isolation innerhalb des Acess Points

Standardmäßig können alle Clients eines Access Points direkt miteinander kommunizieren. Je nach Anwendungsfall kann dies unerwünscht sein.

5.5.1 Isolieren der Funk-Clients

- Wählen Sie die Registerkarte *Network* –> Registerkarte *WiFi* –> Registerkarte *radio0* (oder klicken Sie auf die Schaltfläche *Edit* für *radio0*)
- In der Box *Interface configuration*
  - Wählen Sie die Registerkarte *Advanced settings*
  - Aktivieren Sie das Kontrollkästchen *Separate clients*
- Klicken Sie auf die Schaltfläche *Save & Apply*
- Machen Sie dasselbe für das andere Funkmodul

5.5.2 Beschränkung des Zugriffs von lokalen Ports auf bestimmte Schnittstellen

- Wählen Sie die Registerkarte *System* Registerkarte *Administration*
- In der Box *Dropbear Instance*
  - Klicken Sie auf die Funkmodul-Schaltfläche *lan*
  - [Deaktivieren sie die Funkmodul-Schaltfläche *unspecified*]
- Klicken Sie auf die Schaltfläche *Save & Apply*

Dies betrifft nur den genannten Port. Zum Schutz weiterer Ports vor WLAN-Zugriffen, benutzen Sie die Schaltfläche *Add*.

Beachten Sie, dass alle Schnittstellen, die im Feld *lan* aufgeführt sind, auf den jeweiligen Socket zugreifen dürfen.

6 DAS WEB-INTERFACE

Die meisten Seiten der Weboberfläche befassen sich mit der Konfiguration der CyBox AP 2. Viele dieser Seiten zeigen einige der folgenden Schaltflächen:

- `Reset`: Durch Klicken auf diese Schaltfläche werden die nicht gespeicherten Eingabefelder der aktuellen Seite auf die Werte zurückgesetzt, die sie vor dem Ändern hatten.
- `Save`: Diese Schaltfläche kopiert die geänderten Eingabefelder der aktuellen Seite in einen Zwischenspeicher. Er sammelt Änderungen, ohne sie auf die CyBox AP 2 anzuwenden. Dies ist wichtig, da einige Änderungen - wenn sie eigenständig angewendet werden - die IP-Verbindung zwischen Host und CyBox AP 2 unterbrechen können.

  Wenn Sie auf diese Schaltfläche klicken, wird oben links eine Benachrichtigung über die Anzahl der Änderungen angezeigt, die die Anzahl der zu ändernden Zeilen in den Konfigurationsdaten angibt. (Der tatsächliche Text in dieser Meldung ist etwas irreführend: er behauptet, die Anzahl der „ungespeicherten Änderungen“ anzugeben, meint aber eigentlich die Anzahl der gespeicherten, aber noch nicht angewendeten neuen Konfigurationszeilen).

  Es ist zu beachten, dass gespeicherte Daten nicht mehr der Schaltfläche *Reset* unterliegen. Vielmehr bleiben gespeicherte Änderungen - wenn sie nicht übernommen werden - solange erhalten, bis Sie auf die Schaltfläche `Save & Apply` oder die Schaltfläche `Revert` (siehe unten) klicken oder die CyBox AP 2 neu startet. Die Konfiguration ist noch nicht abgeschlossen, solange die Anzahl der Änderungen ungleich Null ist.
- `Revert`: Wenn Sie auf die Meldung „Change Count“ klicken, öffnet sich ein zusätzliches Fenster, in dem die Daten genau so angezeigt werden, wie sie in die zugehörigen Konfigurationsdateien eingegeben würden. Dieses Fenster enthält eine Schaltfläche mit dem Namen `Revert`. Wenn Sie darauf klicken, werden die gespeicherten Änderungen ungültig und die Anzahl der Änderungen wird auf Null gesetzt.
- `Save & Apply`: Diese Schaltfläche führt den Vorgang *Save* aus (siehe oben), ändert die Konfigurationsdaten entsprechend den gespeicherten Änderungen und löscht die Änderungsanzahl. Bitte beachten Sie, dass `Revert` und `Reset` diese Änderungen nach einem *Save & Apply*-Vorgang *nicht* rückgängig machen können! Abhängig von den geänderten spezifischen Parametern werden die Netzwerkschnittstellen mit den neuen Daten neu initialisiert. Infolgedessen muss der host-seitige Browser möglicherweise eine neue IP-Adresse verbinden, um auf den CyBox AP 2 zuzugreifen.
- *Submit*: Einige Seiten bieten eine einzige *Submit* -Schaltfläche anstelle der oben genannten. Im Wesentlichen führt *Submit* einen sofortigen *Save*-Vorgang aus. Dadurch wird die Anzahl der Änderungen in der oberen linken Ecke des Bildschirms erhöht. Der Vorgang *Save* findet auch statt, wenn Sie auf spezielle Schaltflächen wie *Add new interface* oder *Setup DHCP Server* klicken. Auch hier ändert sich die Anzahl der Änderungen. In diesen Fällen ist *Save & Apply* erforderlich, um den Vorgang abzuschließen.
- Schaltflächen mit dem Namen `Enable` oder `Disable` führen zu einer sorfortigen Ausführung.

6.1 Netzwerk

6.1.1 Interfaces

6.1.1.1 DHCP-Server pro Interface

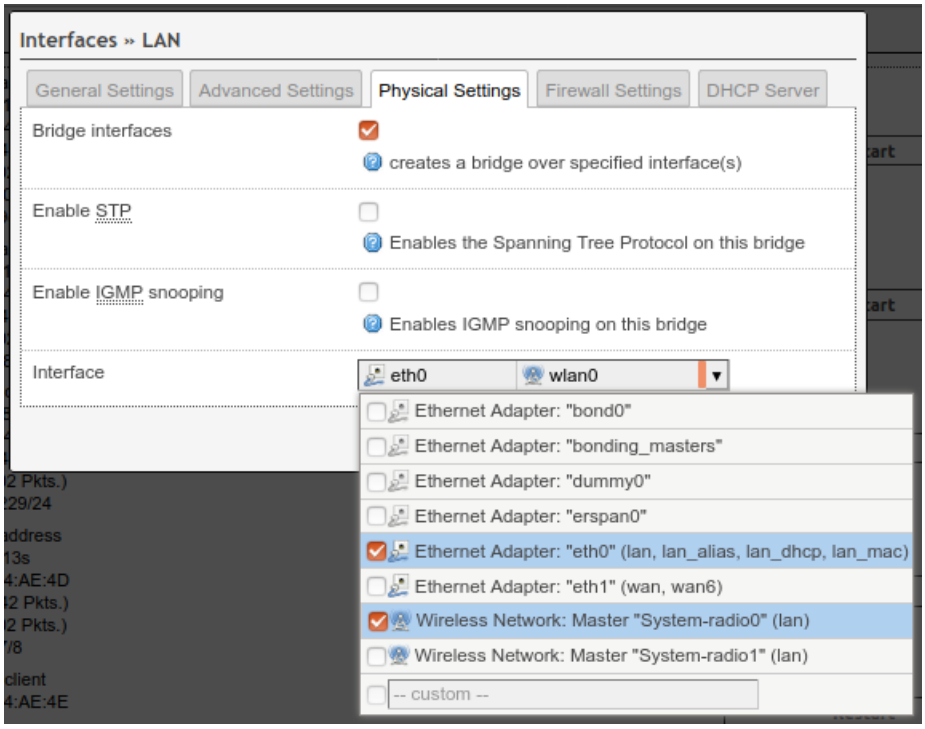
Auf dem Gerät kann ein DHCP-Server laufen, der IPv4-Adressen an WLAN-Clients vergibt. Er wird aktiviert, indem Sie das Häkchen bei *Disable DHCP for this interface* entfernen. Oft wird DHCP jedoch von einem dedizierten DHCP-Server auf dem Backbone verwaltet und nicht direkt auf dem Access Point. In diesem Fall muss der DHCP-Server auf dem Access Point deaktiviert werden.

6.1.1.2 Bridges

Physische Netzwerkschnittstellen können überbrückt werden, um einen „Software-Ethernet-Switch“ zu bilden. Durch die Überbrückung der LAN 1-Schnittstelle mit einer Funk-Schnittstelle können WLAN-Clients beispielsweise mit LAN-Clients kommunizieren, als wären sie über einen Switch verbunden.

Zum Einrichten einer Bridge verwenden Sie die Registerkarte Network → Interfaces → LAN → section Common Configuration → Physical Settings. Überprüfen Sie die Bridge-Schnittstellen und schließen Sie alle *Interfaces* ein, die zur neuen Bridge-Schnittstelle gehören sollen.

Das Beispiel Bridge-Interface-Setup zeigt eine Bridge mit „Ethernet Adapter: eth0“ und „wlan0“ (Wireless Network: Master „System-radio0“).

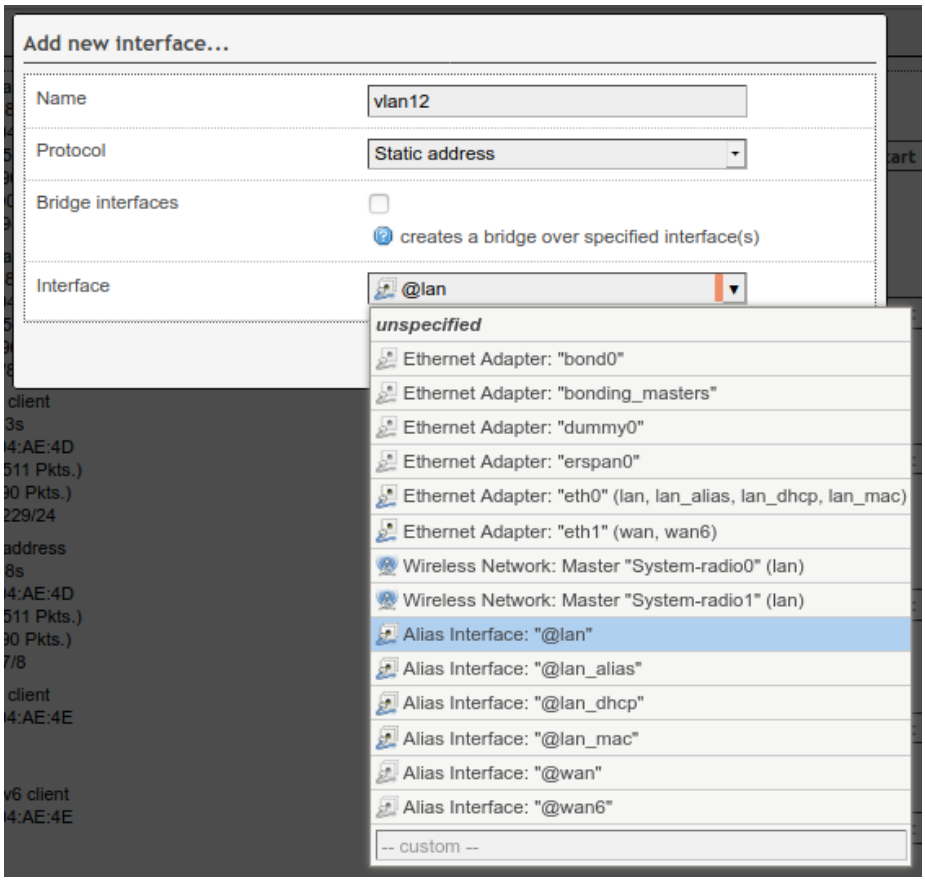


Bridge-Interface-Setup

Hinweis: Physische Schnittstellen wie eth0 oder wlan0, die zu einer Netzwerkschnittstelle wie z.B. LAN gehören, dürfen sich nicht in einer anderen Netzwerkschnittstelle befinden.

6.1.1.3 VLAN

Um das VLAN-Tagging (virtuelles LAN, das hauptsächlich für logische Subnetze verwendet wird, die auf realen LANs basieren) zu aktivieren, muss eine neue benutzerdefinierte Schnittstelle für das *LAN* eingerichtet werden. Die VLAN-Schnittstellen werden z.B. „eth0.12“ genannt. In diesem Beispiel ist „12“ das zu verwendende VLAN-Tag.



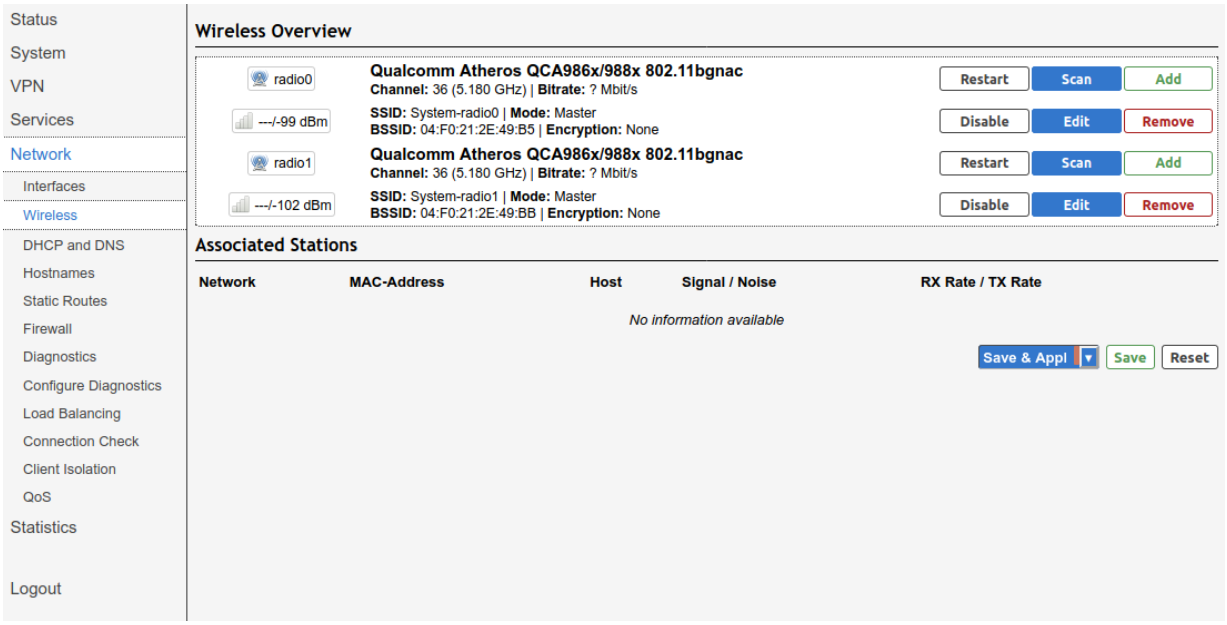
VLAN-Interface-Setup

Verwenden Sie *eth0.X* als benutzerdefinierte Schnittstelle und deaktivieren Sie *eth0* wie im obigen Dialog angezeigt.

WARNUNG: Nach dem Speichern und Anwenden der Änderungen wird die Netzwerkausgabe auf *eth0* mit Ihrem VLAN-Tag versehen, und auf den AP kann nicht mehr über ein normales Netzwerk zugegriffen werden. Sie müssen das VLAN-Tagging auf der Hostschnittstelle aktivieren oder eine Verbindung zu einem Switch herstellen, der dieses VLAN-Tag verarbeiten kann, um auf den AP zugreifen zu können.

6.1.2 WLAN

Funkmodule sind standardmäßig deaktiviert, um einen fehlerhaften WLAN-Betrieb zu vermeiden. Verwenden Sie `Network` → `Wireless` → `Edit` , um das Konfigurationsmenü aufzurufen. Details zur WLAN-Konfiguration finden Sie im nächsten Abschnitt. Aktivieren Sie nach der Konfiguration die Schnittstellen mit `Enable`.



Übersicht der Funkmodule

Das Beispiel zeigt eine CyBox AP 2 mit zwei installierten Funkmodulen. Je nach Hardware können auch andere Konfigurationen angezeigt werden.

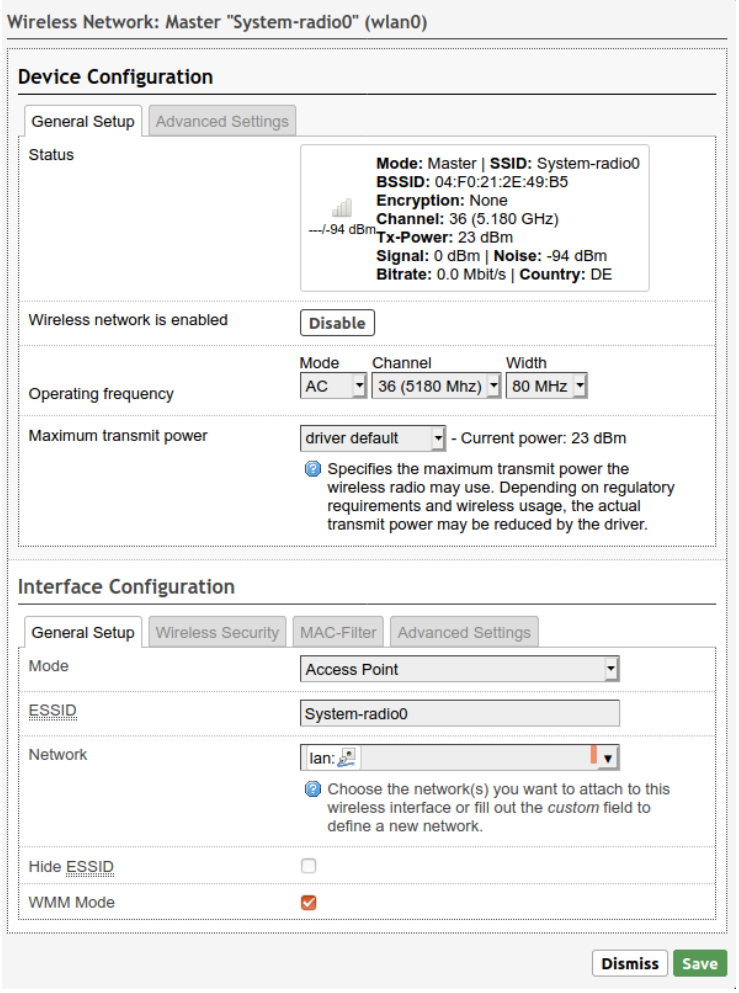
Nachdem Sie das Funkmodul aktiviert haben, können Sie die physikalischen Einstellungen konfigurieren. Durch Anklicken von `Network` → `Wireless` → `Edit` gelangen Sie in das Menü ‚*Device Configuration*‘.

6.1.2.1 Kanal, Wireless-Modus, HT-Modus, Energieeinstellungen

In den erweiterten Einstellungen können Sie das entsprechende Land im Pulldown-Menü auswählen. Drücken Sie nach einer Länderänderung die Schaltfläche *Save & Apply*, aktualisieren Sie die Browserseite und starten Sie neu.

Haftungsausschluss: Die Funk-Konfiguration muss den örtlichen Vorschriften entsprechen. Die Obergrenze der Sendeleistung muss korrekt eingestellt sein („Sendeleistung“). Dabei wird ein Antennengewinn nicht berücksichtigt. Wenn die Regelung beispielsweise eine maximale Leistung von 15 dBm vorschreibt und der Antennengewinn 5 dBm beträgt, müssen Sie die Sendeleistung auf einen Wert von 10 dBm oder darunter einstellen.

Im *General Setup* können Sie den Wireless-Modus, den HT-Modus und den Kanal konfigurieren. Der Wireless-Modus kann auf jeden vom Funkmodul unterstützten 802.11-Standard erzwungen werden. Die Kanalauswahl wird an den gewählten Funkmodus angepasst. Die Kanalkonfiguration kann auf Auto eingestellt werden, dies verlangsamt jedoch die WLAN-Aktivierung und erfordert einen Neustart, um ordnungsgemäß zu funktionieren. Daher wird empfohlen, einen definierten Kanal auszuwählen.



Funkmodulkonfiguration

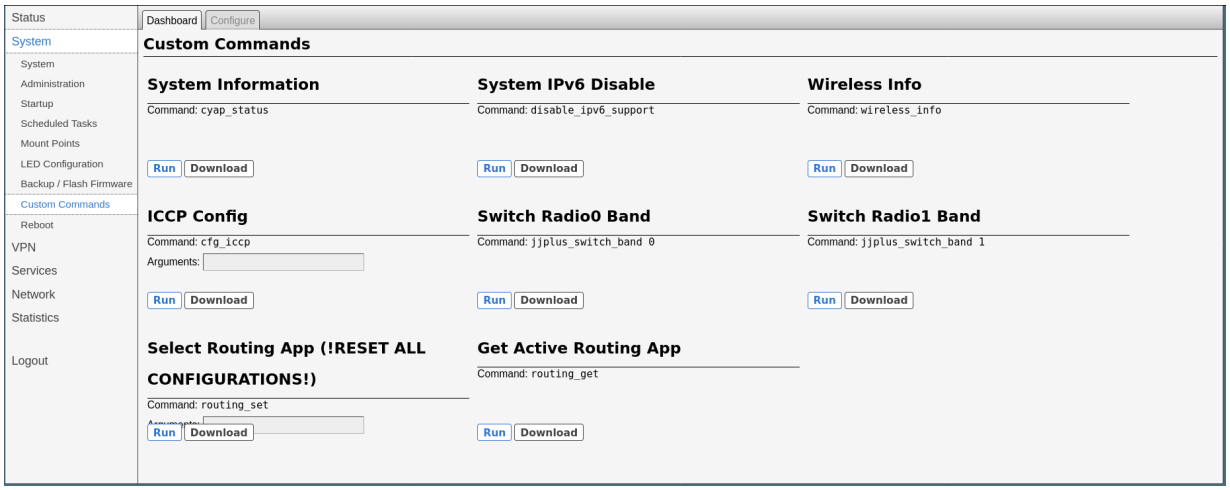
Nachdem das Gerät aktiviert wurde, sollte der Funkstatus überprüft werden, ob die ausgewählte Kanal/Modus-Kombination funktioniert.

6.1.2.2 Funkbandkonfiguration für Modelle mit Antennen-Combiner

Wenn das System mit einem Antennen-Combiner ausgestattet ist (z.B. mit zwei Funkmodulen (WLE-900), aber nur drei Antennen), können die Frequenzbänder 2,4 GHz und 5 GHz nicht für jedes Funkmodul frei konfiguriert werden. Das erste Funkmodul radio0 muss das Band 2,4 GHz und das zweite Funkmodul radio1 das 5-GHz-Band verwenden. Eine falsche Funkbandkonfiguration in der Software ist möglich. Dies führt jedoch dazu, dass an den Antennenports keine Ausgangsleistung ankommt.

6.1.2.3 Bandkonfiguration der JJPlus-Funkkarte

Wenn das System mit einem **JJPlus Wave-2**-Funkmodul ausgestattet ist, können die Frequenzbänden 2,4 GHz und 5 GHz nicht „on the fly“ (im laufenden Betrieb, zur Laufzeit) im Funkkonfigurationsmenü umgeschaltet werden. Nach einem *Factory Reset* sind die Funkmodule für 5 GHz als Standardband konfiguriert. Um auf das 2,4-GHz-Band umzuschalten, muss ein **Custom Command => Switch RadioX Band** ausgeführt und danach ein Systemneustart ausgelöst werden. Der 2,4-GHz-Modus wird dann dauerhaft im Konfigurations-Backup-Archiv gespeichert. Durch erneutes Ausführen der benutzerdefinierten Befehlsschaltfläche wird von 2,4 GHz auf 5 GHz und umgekehrt umgeschaltet. Der ausgewählte Modus wird immer im Konfigurations-Backup-Archiv gespeichert. Beachten Sie, dass eine Bandumschaltung das ausgewählte RadioX immer *deaktiviert*. Nach dem Neustart muss das ausgewählte RadioX erneut aktiviert und der Kanal/die Bandbreite konfiguriert werden.



Umschalten des JJPlus Wave-2-Frequenzbandes

6.1.2.4 ESSID, WDS-Modus, Client Separation

Die ESSID wird für WLAN-Clients verwendet, um das WLAN anhand des Namens auszuwählen. Richten Sie im *General Setup* der *Interface Configuration* einen ESSID-Namen für das drahtlose Netzwerk ein und verwenden Sie den Modus *Access Point*.

Ein Wireless Distribution System (WDS) kann mithilfe von zwei Access Points mit derselben ESSID eingerichtet werden, einer im Modus „Access Point (WDS)“ und der andere im Modus „Client (WDS)“. Dieser Modus ist für das Inter Carriage Connection Protocol (ICCP) erforderlich.

In öffentlichen Access-Point-Umgebungen sollte die Client-zu-Client-Kommunikation durch Aktivieren des Kontrollkästchens `Interface Configuration` → `Advanced Settings` → `Isolate Clients` verhindert werden. Beachten Sie, dass diese Konfiguration nur die Kommunikation zwischen Clients verhindert, die mit demselben Zugriffspunkt verbunden sind. In einem Backbone mit vielen Access Points, die die gleiche SSID haben, wird eine zusätzliche „Client Isolation“-Funktion zwischen APs benötigt (siehe 6.1.2.8 Multi-AP Client Isolation).

6.1.2.5 Verschlüsselung

Auf der Registerkarte `Wireless Security` können Sie einen Sicherheitsmodus auswählen. Die folgenden Modi werden unterstützt:

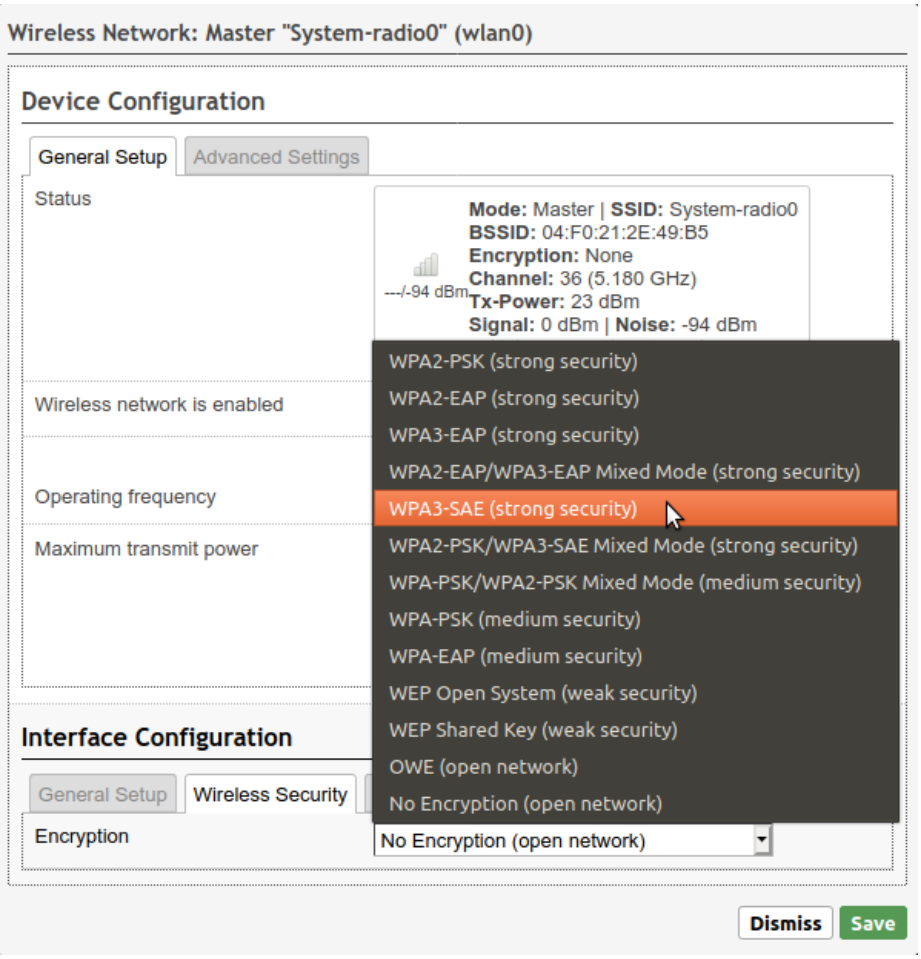
- WPA3 (hohe Sicherheit)
    - WPA3-SAE: „Persönlicher Modus“ mit einem Schlüssel (Passwort) für den Zugriff.
    - WPA3-EAP: „Unternehmensmodus“ unter Verwendung eines RADIUS-Servers zur Client-Authentifizierung.
- WPA2 (hohe Sicherheit)
    - WPA2-PSK: „Persönlicher Modus“ mit einem Passwort für den Zugriff. Beachten Sie, dass die Verschlüsselung „TKIP“ als unsicher angesehen wird und stattdessen CCMP verwendet werden sollte
    - WPA2-EAP: „Unternehmensmodus“ unter Verwendung eines RADIUS-Servers für die Client-Authentifizierung.
- WPA (mittlere Sicherheit)

- WPA-PSK: „Persönlicher Modus“ mit einem Passwort für den Zugriff. Beachten Sie, dass die Verschlüsselung „TKIP“ als unsicher angesehen wird und stattdessen CCMP verwendet werden sollte.
- WPA-EAP: „Unternehmensmodus“ unter Verwendung eines RADIUS-Servers für die Client-Authentifizierung.

- WEP (schwache Sicherheit)
  - WEP Gemeinsamer Schlüssel
  - WEP-EAP Offenes System
- OWE (offen, verschlüsselt)
  - OWE: Der Modus „Opportunistic Wireless Encryption“ erfordert kein Passwort, dennoch wird der WLAN-Verkehr verschlüsselt. Dieser Modus ist für öffentliche Access Points gedacht.
- Keine Verschlüsselung (offen):
  - Der WLAN-Verkehr ist überhaupt nicht gesichert.

Zusätzlich können einige dieser Modi kombiniert werden („mixed mode“). Dies ermöglicht es einem Access Point, mehrere Modi zu unterstützen und dabei neuere Verschlüsselungsstandards zu unterstützen, während ältere Clients weiterhin unterstützt werden. Wenn Sie die CyBox AP 2 als Client mit einem „mixed mode“ konfigurieren, wird er beide Modi ausprobieren, wenn er sich mit einem Access Point verbindet (normalerweise wird nur der konfigurierte Modus verwendet). Die folgenden Modi können kombiniert werden:

- WPA3 and WPA2 im Unternehmensmodus (EAP)
- WPA3 and WPA2 im persönlichen Modu (PSK bzw. SAE)
- WPA2 and WPA im persönlichen Modu (PSK)



Konfiguration Funkmodule - Verschlüsselungseinstellungen

6.1.2.6 Hotspot 2.0

Die CyBox AP 2 unterstützt Hotspot 2.0 (Release 1), das auf der Registerkarte `Hotspot 2.0` konfiguriert ist.

> **Bemerkung**
>
> Die Registerkarte `Hotspot 2.0` ist nur vorhanden, wenn
>
> - das WLAN als AP konfiguriert ist
> - der Verschlüsselungsmodus nutzt RADIUS (d.h. EAP)
>
> SP/HO

Hotspot 2.0 trennt den Hotspot-Betreiber von den Dienstanbietern. Der Hotspot-Betreiber unterhält den Access Point, der Hotspot-2.0-Dienste anbietet, während die Dienstanbieter für die Authentifizierung und Autorisierung der WLAN-Clients verantwortlich sind. Es ist möglich, mehrere Service-Provider auf einem einzigen Access Point zu konfigurieren.

Jeder Hotspot-Betreiber hat einen oder mehrere Domain-Namen, die in der Einstellung `Domain Names` konfiguriert werden können.

Service-Provider werden durch einen der folgenden Punkte gekennzeichnet:

- `Consortium IDs`: Numerische Werte, die von der IEEE zugewiesen werden. Jede ID benennt ein Konsortium aus mehreren Service-Providern.
- `NAI Realms`: Die Domänennamen der Service-Provider. Optional kann das Authentifizierungsschema an jeden Namen angehängt werden. Die WLAN-Clients können diese Informationen abrufen, bevor sie eine Verbindung herstellen.
- `3GPP Cell Identifiers`: Jede Zell-ID besteht aus dem MCC und MNC eines Service-Providers. Ein mobiles Gerät kann nahtlos zwischen Mobilfunknetzen und WLAN wechseln, indem es seinen Mobilfunkanbieter an einem Hotspot 2.0 Access Point identifiziert.

Mindestens einer dieser drei Parameter muss konfiguriert sein.

Der `Operator Friendly Name` ist der Name des Access Point-Betreibers. Er soll den menschlichen Benutzern von WLAN-Clients angezeigt werden. Es können mehrere Einträge konfiguriert werden, um den Namen in verschiedenen Sprachen darzustellen.

Die Einstellungen `Venue Group` und `Venue Type` klassifizieren den Typ des Veranstaltungsortes, an dem der Access Point installiert ist. Dies könnte beispielsweise ein Café sein. Die möglichen Werte sind in IEEE Std 802.11u-2011 definiert.

Der `Venue Name` kann menschlichen Benutzern angezeigt werden. Er kann für mehrere Sprachen konfiguriert werden.

Der `Network Access Type` beschreibt den Typ des angebotenen Netzwerkzugriffs. Das `Internet is available` zeigt an, ob der Internetzugang von diesem Access Point aus verfügbar ist. Beide werden WLAN-Clients angezeigt, bevor sie eine Verbindung herstellen.

Die `ANQP Domain ID` kann verwendet werden, um mehrere Access Points zu gruppieren, die sich im gleichen ESS (Extended Service Set) befinden.

Die Einstellung `Additional ANQP Elements` erlaubt das Hinzufügen von Elementen.

6.1.2.7 WLAN Client-Test

Nachdem die Einrichtung abgeschlossen ist, ist der Access Point bereit, WLAN-Clients mit dem lokalen Netzwerk zu verbinden.

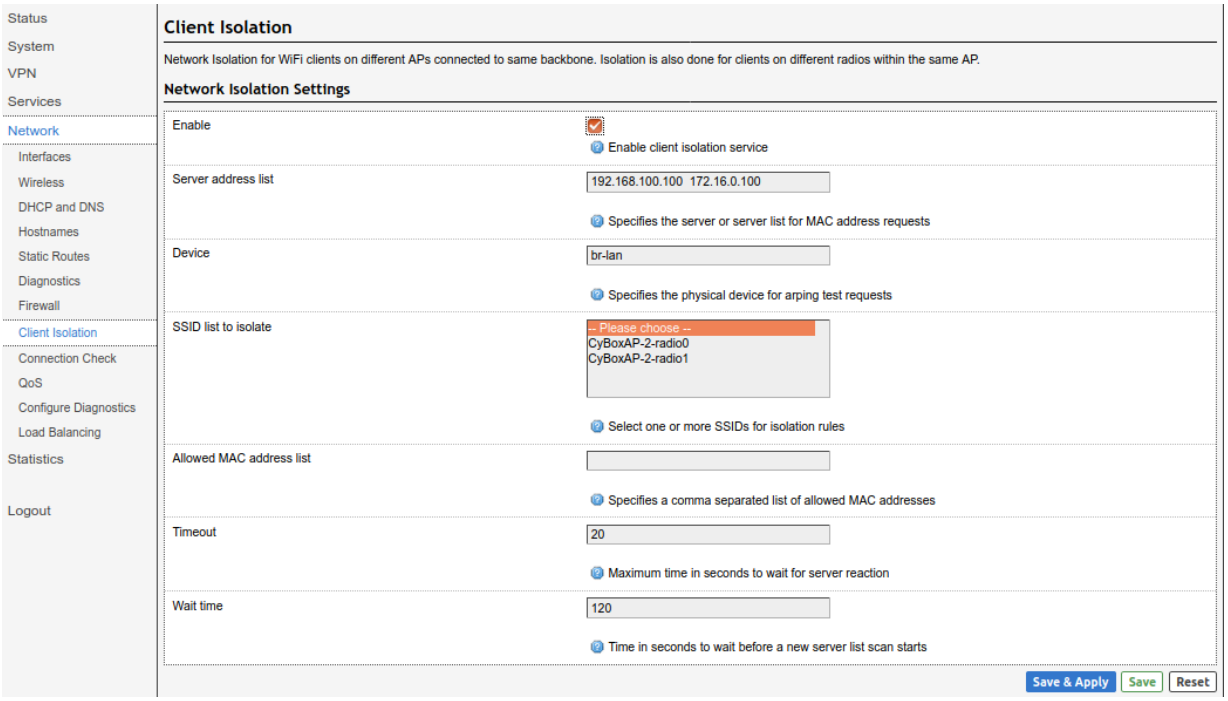
6.1.2.8 Multi-AP Client Isolation

Die Client-Trennung verhindert die direkte Kommunikation zwischen Clients desselben WLAN-Funkmoduls. Wenn jedoch mehr als ein Access Point an dasselbe Kabel-Backbone angeschlossen ist und die WLAN-Clients dasselbe Subnetz verwenden, muss die Client-Isolation auch zwischen den APs aktiviert werden. Dies gilt auch, wenn die CyBox AP 2 mehrere APs auf verschiedenen WLAN-Modulen betreibt, die verbunden sind (z. B. unter Verwendung einer Bridge). Die Isolierung erfolgt auch für Clients auf verschiedenen Funkmodulen innerhalb desselben Access Points.

Um die Multi-AP-Client-Isolation zu verwenden, müssen alle APs denselben Server und denselben Schnittstellennamen verwenden. (Der Netzwerkverkehr kann mit einer Konfiguration für ‚ebtables' auf FORWARD-Regeln eingeschränkt werden, die von der Funktion ‚Client-Isolation' verwaltet wird).

Für die Client-Isolation über APs markieren Sie Network → Client Isolation → Enable und geben dann Parameter für Ihre Konfiguration ein.

Der folgende Screenshot zeigt eine Konfiguration, bei der die Serveradresse in den Parametern der Lan-Schnittstelle eingestellt ist (unter '*Network*' →'*Interfaces*'). Wenn die Schnittstelle als Bridge eingerichtet ist, lautet der entsprechende Bridge-Name immer 'br-<*original_interface_name*>'



Client-Isolation über Access Points hinweg

6.1.2.9 Verbindungstest

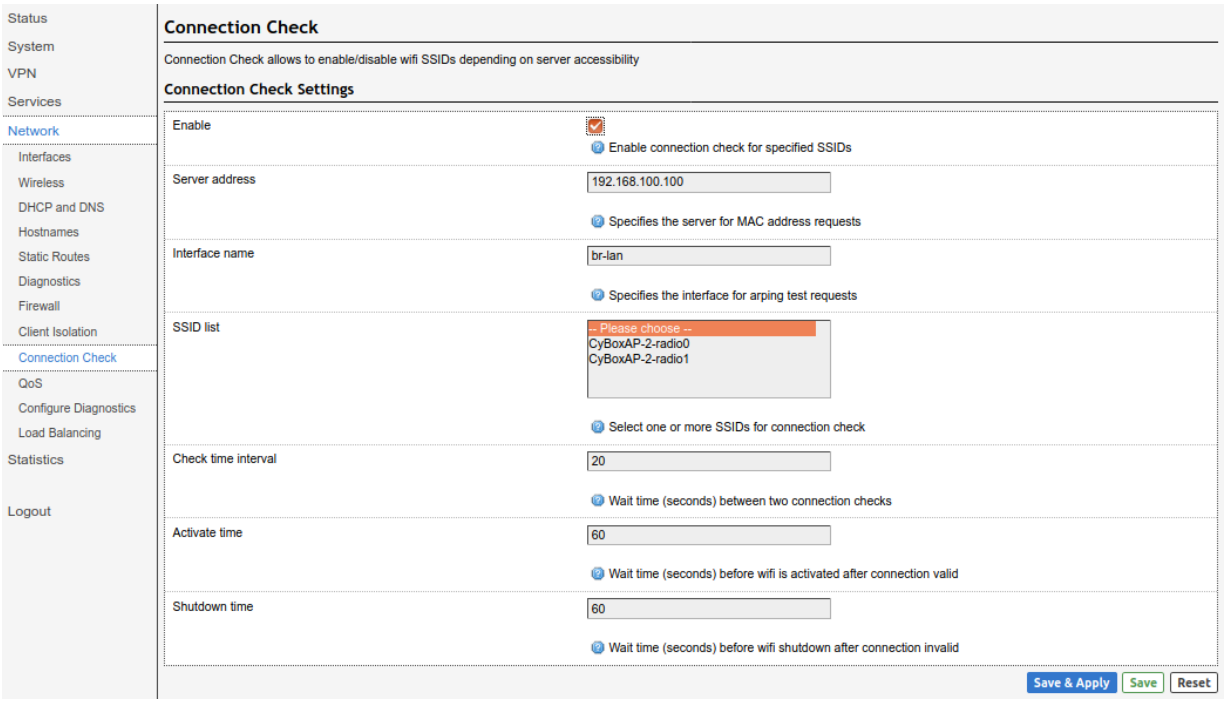
Mit dem Verbindungstest-Service können WLANs deaktiviert werden, wenn keine Internetverbindung möglich ist. Dies kann das Benutzererlebnis verbessern, da vermieden wird, dass eine Verbindung zu einem WLAN hergestellt wird, das keine Internetverbindung bietet.

Die Verbindungsüberprüfung funktioniert, indem ein *arping* an den Server gesendet wird. Wenn der Server nicht erreichbar ist, wird das WLAN deaktiviert. Andernfalls wird das WLAN aktiviert. Der Dienst kann auf folgender Seite konfiguriert werden `Network` → `Connection Check` (siehe unten Abbildung „Deaktivieren Sie SSIDs, wenn der Server nicht erreichbar ist“). Das Kontrollkästchen `Enable` aktiviert oder deaktiviert ihn.

Der Parameter `Server address` bestimmt, welche Adresse abgefragt wird, um festzustellen, ob die Verbindung fehlerfrei ist. Der Parameter `Interface name` gibt an, welche Schnittstelle für das Arping verwendet wird. Beachten Sie, dass es sich hierbei um eine physikalische Schnittstelle handelt, wie z.B. `br-lan` or `eth0`.

In der `SSID list` können die kontrollierten SSIDs ausgewählt werden. Die ausgewählten SSIDs werden vom Dienst aktiviert oder deaktiviert, während die anderen unbeeinflusst bleiben.

Die Verbindung wird alle `Check time interval` Sekunden überprüft. Die ausgewählten SSIDs sind deaktiviert, wenn die Verbindung für mindestens `Shutdown time` Sekunden unterbrochen wurde, und sie werden wieder aktiviert, wenn die Verbindung für mindestens `Activate time` Sekunden fehlerfrei war. Beachten Sie, dass die beiden letzteren auf der Granularität von `Check time interval`:. Wenn das `Check time interval` → 15s und die `Activate time` → 20s beträgt, werden die WLANs nach der 2. erfolgreichen Prüfung, also nach 30s, aktiviert.



Deaktivieren Sie SSIDs, wenn der Server nicht erreichbar ist

6.1.2.10 Access Point-Scanning-Service (Funküberwachung)

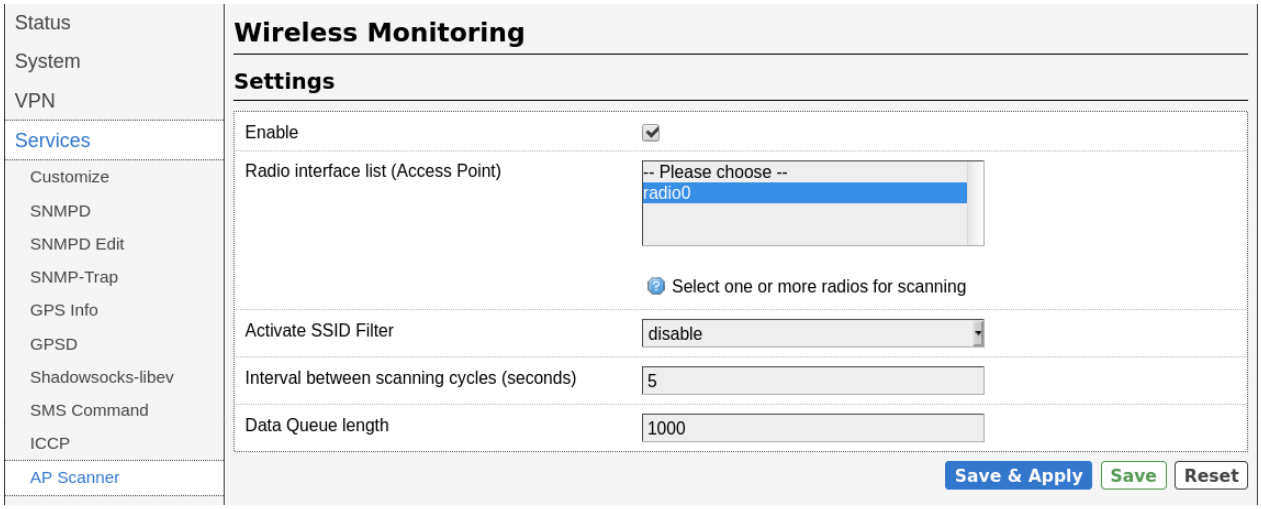
Meldung von nahegelegenen APs an interessierte Kreise

> **Wichtig**
>
> Eine **Muss**-Voraussetzung für die Nutzung dieses Dienstes ist, dass mindestens ein Funkmodul im AP-(Access Point)-Modus verfügbar ist. Bitte stellen Sie sicher, dass diese Konfiguration abgeschlossen ist und ausgeführt wird, **bevor** Sie diesen Dienst aktivieren. Andernfalls können keine Scanergebnisse erhalten werden.

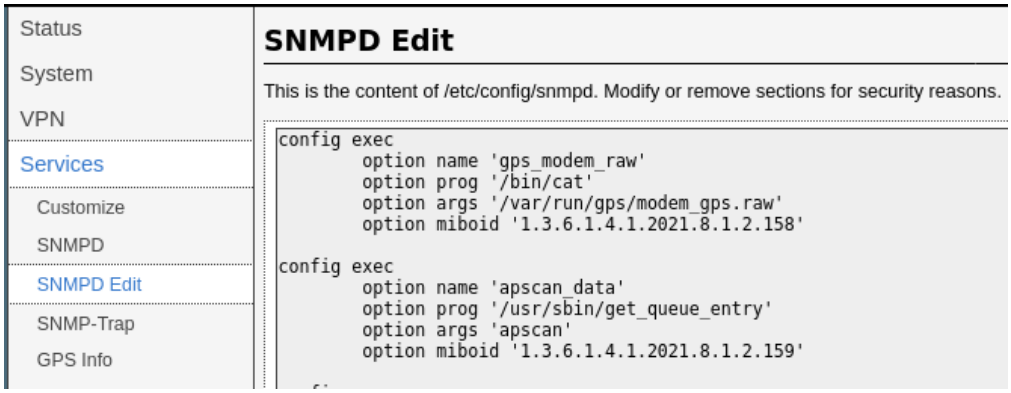
Da der Dienst aktiviert (freigeschaltet) ist, wird das Scannen kontinuierlich im Hintergrund durchgeführt. Alle Kanäle des/der ausgewählten Funkmoduls/Funkmodule werden nacheinander gescannt. Die Scanergebnisse werden in einer temporären FIFO-Warteschlange gespeichert und können jederzeit abgerufen werden.

Der Scan-Service kann über UCI bzw. LUCI konfiguriert werden. Auf einer separaten Seite (Services -> AP Scanner) können die Funkmodule konfiguriert werden, die zum Scannen verwendet werden. Auch das Intervall zwischen den Scan-Zyklen und der maximalen Länge der Warteschlangen kann konfiguriert werden.

> **Wichtig**
>
> Die Systemlast und der Netzwerkverkehr, die durch SNMP-Aufrufe verursacht werden, können mithilfe von SSID-Filterparametern minimiert werden. Solange der SSID-Filter aktiviert ist, werden nur Einträge, die mit dem vordefinierten Filter übereinstimmen, in einer Ergebniswarteschlange gespeichert.



Die Scan-Ergebnisse können über eine SNMP-Anfrage abgerufen werden. Die Konfiguration der Anfrage kann auch über die UI-Seite (Services->SNMPD Edit) erfolgen.



Abrufen des Warteschlangeneintrags vom Remote-Host

```
~# 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:
"00:15:61:20:AC:8A;CyBoxGW-P-radio1;04:F0:21:3F:2E:AA;36;-27;2020-05-06 13:20:17"
```

Im Falle einer leeren Warteschlange wird als Antwort ein „nil“-Wert ausgegeben.

```
~# 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"
```

Wichtig

Sobald die Warteschlange die konfigurierte Maximallänge erreicht hat, wird bei jedem neuen Eintrag in die Warteschlange der „älteste“ Eintrag verworfen!

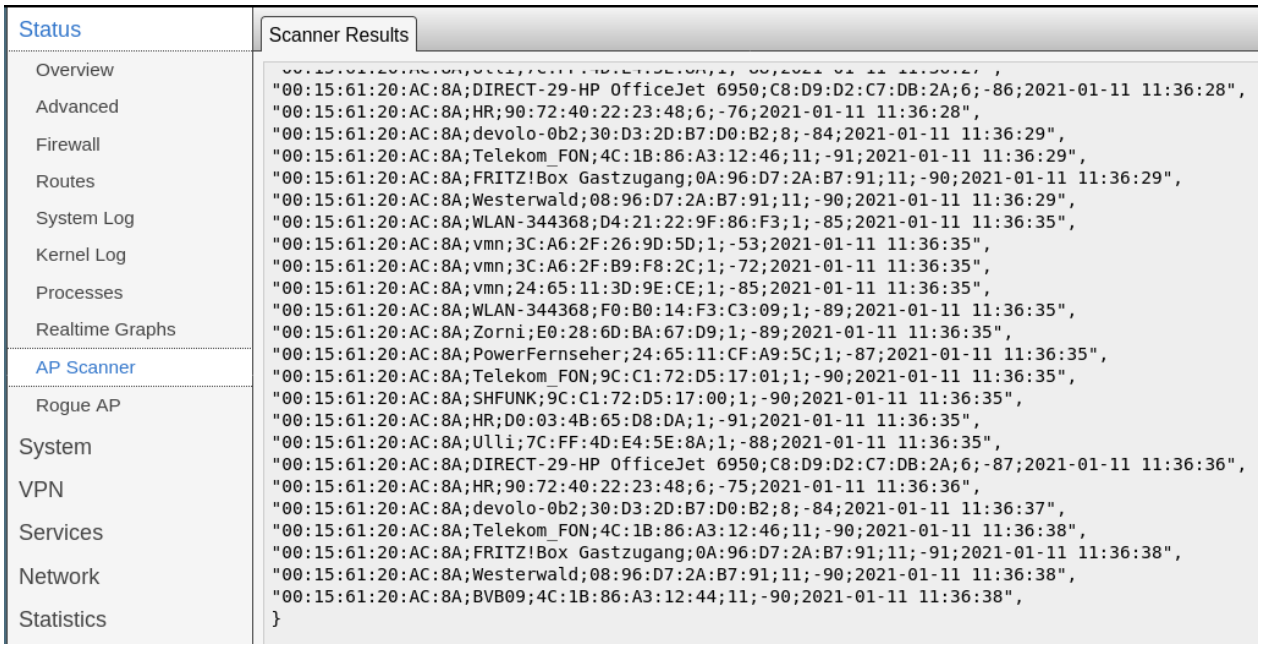
Wie kann man Datenverluste vermeiden?

1. Erhöhen Sie die maximale Warteschlangenlänge.
2. Sammeln Sie häufiger abgetastete Daten, z.B. einmal pro Sekunde (snmp-Anfrage)

Die Scanergebnisse werden im CSV-Format gespeichert:

- S_BSSID (MAC des Scanner-Funkradios)
- SSID (der Name)
- BSSID (der MAC)
- Kanal
- Signal-Level
- Zuletzt gesehener Zeitstempel „last seen“

Der aktuelle Status der Warteschlange (entries) kann auch auf der UI-Seite (Status -> AP Scanner) ermittelt werden.



6.1.2.11 Client Counting Service

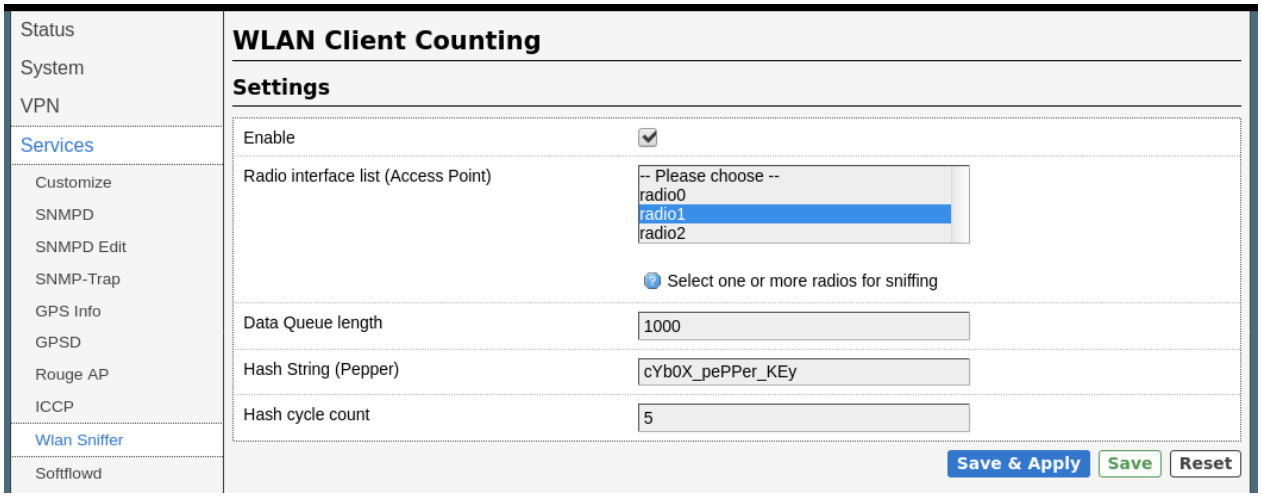
Meldung von nahegelegenen Kunden an interessierte Parteien

Wichtig

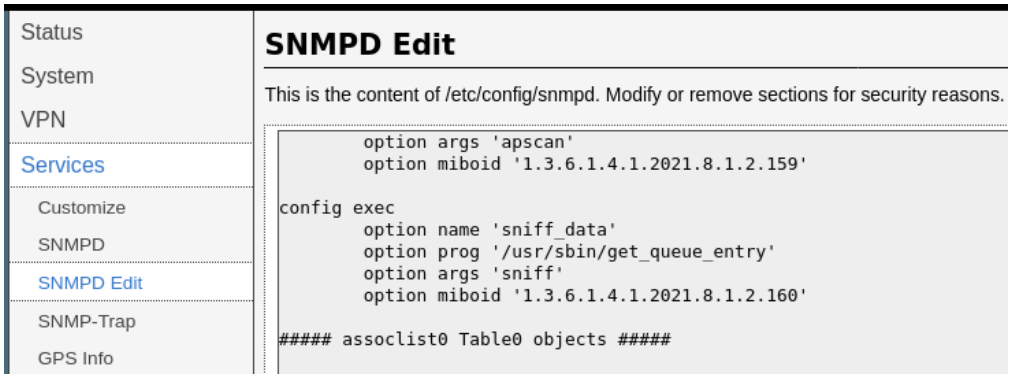
Eine **Muss**-Voraussetzung für die Nutzung dieses Dienstes ist, dass mindestens ein verfügbares Funkmodul im AP-(Access Point)-Modus läuft. Bitte stellen Sie sicher, dass diese Konfiguration abgeschlossen ist und ausgeführt wird, **bevor** Sie diesen Service aktivieren. Andernfalls können keine Sniffing-Ergebnisse erzielt werden.

Da der Dienst aktiviert (freigegeben) ist, erfolgt das Sniffing kontinuierlich im Hintergrund. Für die ausgewählte(n) Funkschnittstelle(n) wird ein spezielles Überwachungsgerät erstellt. Daten, die von der Funkschnittstelle (AP) empfangen werden, werden ebenfalls über das Überwachungsgerät übertragen. Testanforderungen, die von Clients rund um das Überwachungsgerät gesendet werden, werden zur eindeutigen Identifizierung des Clients verwendet. „Ausgeschnüffelte“ (sniffed) personenbezogene Daten (MAC und SSID) müssen gemäß den Anforderungen der Datenschutzverordnung (DSGVO) geschützt werden. Der Verschlüsselungsalgorithmus verwendet einen zusätzlichen String (Pepper), der vom Benutzer konfiguriert wird, um bessere Anonymisierungsergebnisse zu erzielen. Außerdem gibt es einen Mechanismus, um personenbezogene Daten mehrfach zu verschlüsseln (hash_count). Die Ergebnisse werden in einer temporären FIFO-Warteschlange gespeichert und können jederzeit abgerufen werden.

Der Sniffing-Dienst ist über UCI bzw. LUCI konfigurierbar. Auf einer separaten Seite (Services -> WLAN Sniffer) können Funkmodule konfiguriert werden, die zum Sniffing verwendet werden. Auch die maximale Warteschlangenlänge, zusätzliche String- und Hash-Cycle-Zählwerte können konfiguriert werden.



Die Ergebnisse können über eine SNMP-Anfrage abgerufen werden. Die Abfragekonfiguration kann auch über die UI-Seite (Services->SNMPD Edit) erfolgen.



Abrufen des Warteschlangeneintrags vom Remote-Host

```
~# 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: "radio1;
    c78236b5fb56b9023249e23e94dae7092aaa16f792aa168b21c064713b9883fe;
    n/a;
    -29dBm;
    2020-05-07 09:25:20"
```

Im Falle einer leeren Warteschlange wird als Antwort ein „nil“-Wert ausgegeben.

```
~# 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"
```

Wichtig

Sobald die Warteschlange die konfigurierte Maximallänge erreicht hat, wird bei jedem neuen Eintrag in die Warteschlange der „älteste“ Eintrag verworfen!

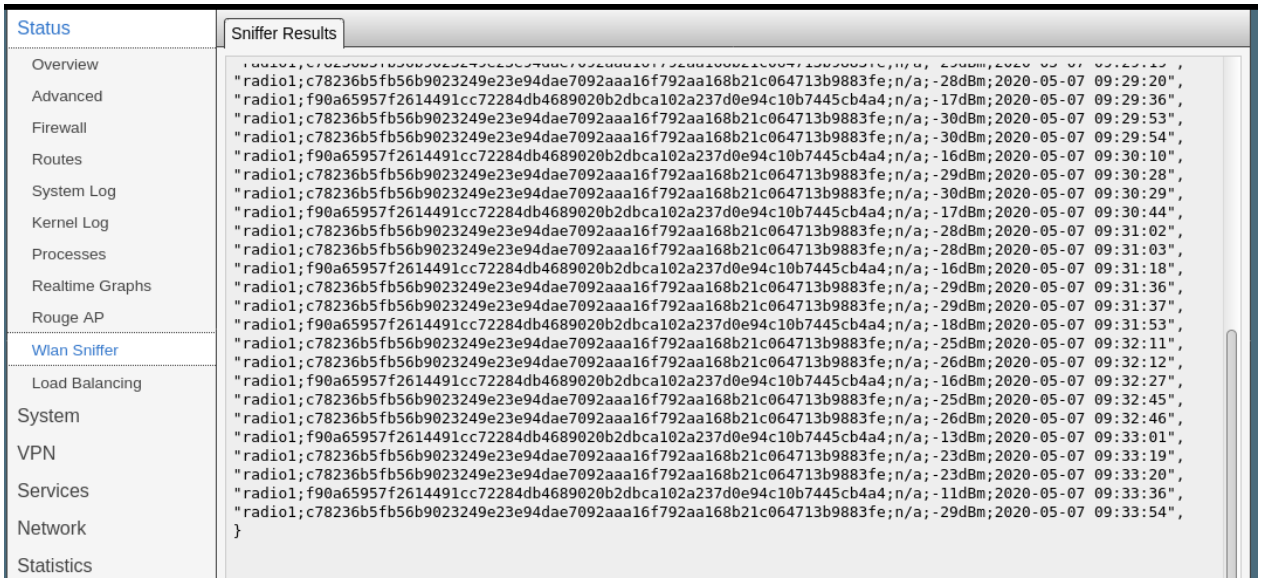
Wie kann man Datenverluste vermeiden?

1. maximale Warteschlangenlänge erhöhen
2. Sammeln Sie abgetastete Daten häufiger, z.B. einmal pro Sekunde (snmp-Abfrage)

Die gesnifften Ergebnisse werden im CSV-Format gespeichert:

- Funkmodul (das zum Sniffing verwendet wird, z.B. radio0)
- MAC
- SSID (n/a für leeren SSID)
- RSSI (Signallevel in dBm)
- Zeitstempel „last seen“

Der aktuelle Status der Warteschlange (Einträge) kann auch auf der UI-Seite (Status -> WLAN Sniffer) ermittelt werden.



6.1.2.12 Rogue-Access Point-Erkennungsservice

Dieser Service dient dem Erkennen nicht autorisierter Access Points in der Nähe und scannt nahegelegene Access Points und klassifiziert sie als „rogue“ oder „not rogue“. Die Rogue-APs werden über SNMP-Traps gemeldet.

> **Wichtig**
>
> Der Algorithmus zur Erkennung von Rogue-APs stützt sich auf den 8 DER FLYING CONTROLLER-MECHANISMUS . Der Erkennungsalgorithmus ist nur auf Geräten aktiv, die im **Controller**-Modus laufen. Da die Auswahl des Controller-Modus zwischen Geräten, die im gleichen Netzwerk (LAN) laufen, automatisch erfolgt, müssen alle potenziellen Kandidaten für die Rogue-AP-Erkennung identisch konfiguriert sein.

Mehrere Geräte können an der Erkennung von Rogue-Access-Points teilnehmen. Jedes Gerät, auf dem der AP-Scan-Service und die Flying-Controller-Dienste ausgeführt werden und das mit dem gemeinsamen drahtgebundenen Netzwerk verbunden ist, kann als Teil des Erkennungsnetzwerks verwendet werden. Alle gescannten Daten der Erkennungsteilnehmer werden vom Controller-Gerät über SNMP-Aufrufe abgefragt und für die Rogue-AP-Erkennung verwendet.

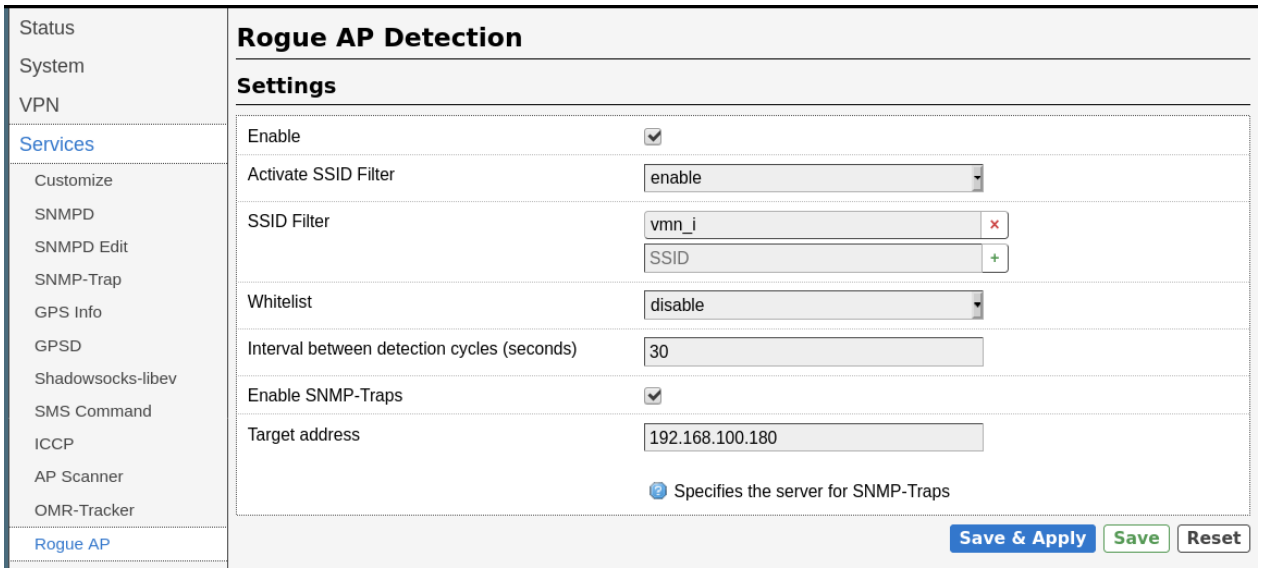
> **Wichtig**
>
> Der Algorithmus zur Erkennung von Rogue-APs basiert auf dem 6.1.2.10 Access Point-Scanning-Service (Funküberwachung) , der auf allen beteiligten Geräten läuft.

Solange ein SSID-Filter aktiviert ist, werden nur Einträge, die dem vordefinierten Filter entsprechen, zur Erkennung herangezogen. Bekannte autorisierte Geräte können mit Hilfe des Whitelist-Parameters auf eine Whitelist gesetzt werden. Teilnehmer des gemeinsamen Netzwerks (d. h. die Worker des Flying-Controller-Mechanismus) werden automatisch in die Whitelist aufgenommen.

Wichtig

Die Systemlast und der Netzwerkverkehr, die durch SNMP-Aufrufe verursacht werden, können mithilfe von SSID-Filterparametern minimiert werden. Dies kann auch für den AP-Scanner-Service erfolgen.

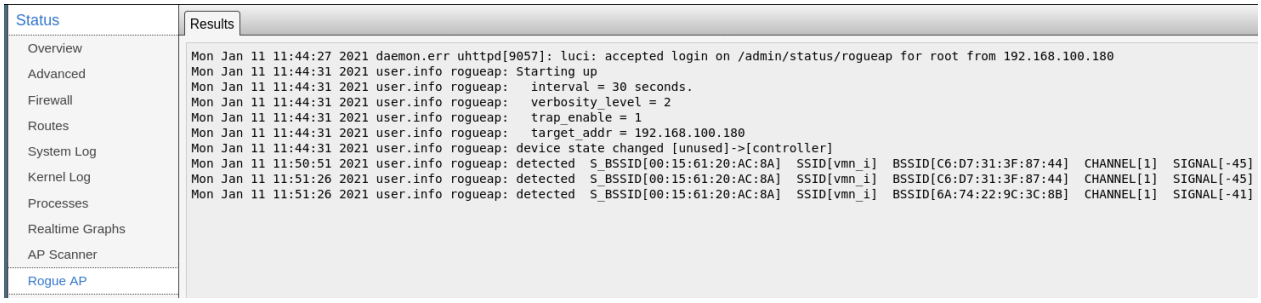
Teilnehmer, die mit dem kabelgebundenen Netzwerk verbunden sind (alle Worker und der Controller selbst), werden vom Dienst automatisch auf eine Whitelist gesetzt und nicht als Rogue-Geräte erkannt. Alle anderen gescannten APs mit der gleichen SSID werden als Rogue deklariert und an einen festgelegten Host gemeldet. Diese Benachrichtigungen können mit dem Parameter „Enable SNMP Traps“ aktiviert werden. Die IP-Adresse des SNMP-Trap-Empfängers kann mit dem Parameter „Target address“ konfiguriert werden.



SNMP-Benachrichtigungen sind innerhalb der ELTEC-MIB definiert und haben folgendes 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::rogueDataSBSSID
```

Statusmeldungen können auf der UI-Seite gefunden werden (Status->RogueAP).



6.1.3 Multi-WAN-Manager (MWAN3)

Der Multi-WAN-Manager (MWAN3) kann gesteuert werden, welche Netzwerkverbindung für den Datenverkehr verwendet werden soll. Dieser Abschnitt verdeutlicht dies am Beispiel von LTE-Uplink-Verbindungen, es können aber auch andere Verbindungen - wie WLAN oder Ethernet - verwendet werden.

Er bietet die folgenden Funktionen:

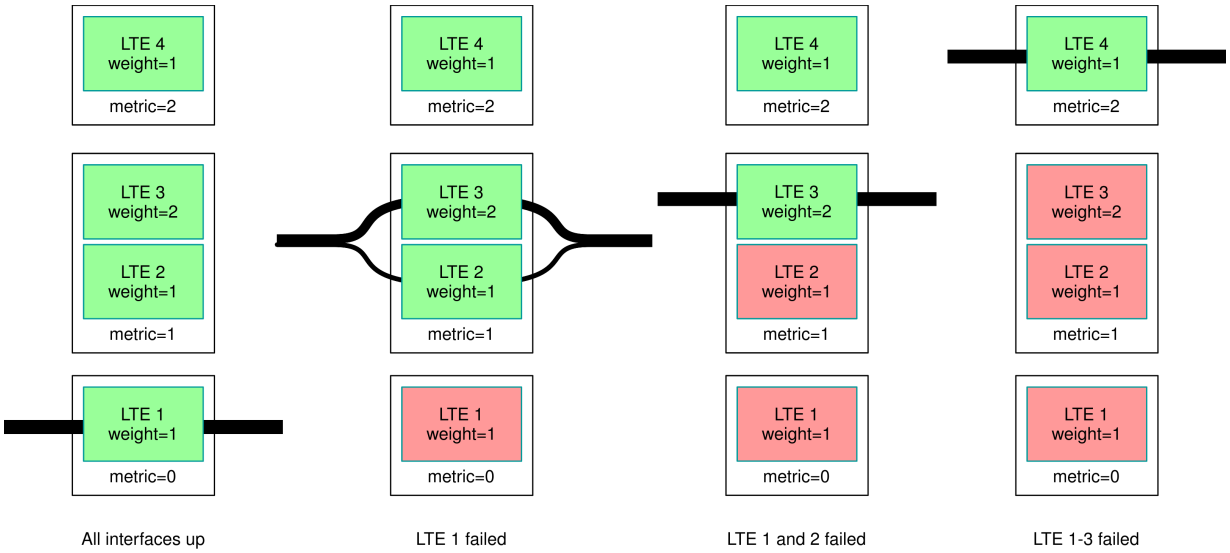
- Überwachung der WAN-Konnektivität durch wiederholte Ping-Tests (ping | arping | httping).
- Routing des ausgehenden Datenverkehrs zu einer anderen WAN-Schnittstelle, wenn die erste WAN-Schnittstelle die Konnektivität verliert, basierend auf der Metrik. Die Verbindung mit der niedrigsten Metrik wird bevorzugt, andere Verbindungen werden nur verwendet, wenn die bevorzugte ausfällt. Schnittstellen, die denselben Metrikwert haben, bilden eine „Gruppe“.
- Lastverteilung des ausgehenden WAN-Verkehrs über mehrere WAN-Schnittstellen basierend auf einer numerischen Gewichtszuweisung. Alle Verbindungen mit der gleichen Metrik („innerhalb der gleichen Gruppe“) werden gleichzeitig verwendet und verteilen den Datenverkehr auf sie. Verbindungen mit höherer Gewichtung bekommen mehr Verkehr zugewiesen..
- Für verschiedene Verkehrsarten können unterschiedliche Richtlinien definiert werden. Beispielsweise könnte der OpenVPN-Verkehr über die erste Verbindung geleitet werden (wobei die anderen Verbindungen nur verwendet werden, wenn sie ausfällt), während der gesamte andere Verkehr über die übrigen Verbindungen geleitet wird (mit Lastausgleich zwischen ihnen).

Load-Balancing benötigt keine Gegenstelle am Boden, es wird komplett vom CyBox AP 2 erledigt. Als solches ist es keine Link-Aggregation. Es verteilt den Verkehr nach Streams, nicht nach Paketen, d. h. ein einzelner Stream kann nicht von mehreren LTE-Verbindungen profitieren. Zum Beispiel kann ein einzelner Download-Stream nur eine LTE-Verbindung nutzen. Mehrere Streams (z. B. generiert von vielen WLAN-Benutzern an Bord eines Zuges) können jedoch über mehrere WAN-Verbindungen verteilt werden, wodurch die Gesamtbandbreite erhöht wird.

Die Abbildung Beispiel Verkehrsfluss im MWAN zeigt eine Beispielkonfiguration und visualisiert die Verkehrsflüsse in verschiedenen Situationen:

- Wenn alle Schnittstellen aktiv sind, wird der gesamte Datenverkehr über die Schnittstelle mit der niedrigsten Metrik geleitet, d. h. LTE 1 (Metrik=0).
- Wenn LTE 1 ausfällt, wird der gesamte Verkehr weiterhin über die betriebsfähigen Schnittstellen mit der niedrigsten Metrik (=1) geleitet. Dies sind nun aber LTE 2 und LTE 3, die sich die gleiche Metrik teilen. Der Verkehr wird auf diese Schnittstellen verteilt (Load-Balancing).
- Wenn LTE 1 und 2 ausfallen, wird der Verkehr über LTE 3 geleitet, da dies nun die betriebsfähige Schnittstelle mit der niedrigsten Metrik ist. Es findet kein Lastausgleich mehr statt, da nur noch eine Schnittstelle verwendet wird.
- Wenn LTE 1-3 ausfallen, wird LTE 4 verwendet. Technisch gesehen ist es die betriebsfähige Schnittstelle mit der niedrigsten Metrik.

Beachten Sie, dass der Lastausgleich zwischen LTE 2 und LTE 3 mehr Verkehr über LTE 3 als über LTE 2 leitet. Das liegt an den unterschiedlichen Gewichten. Die Schnittstelle mit der höheren Gewichtung erhält mehr Datenverkehr. Wenn jetzt ein Lastausgleich stattfindet, haben die Gewichtungswerte keine Auswirkung.



Beispiel Verkehrsfluss im MWAN

6.1.3.1 Funktionen

Das MWAN3-Paket bietet die folgenden Funktionen:

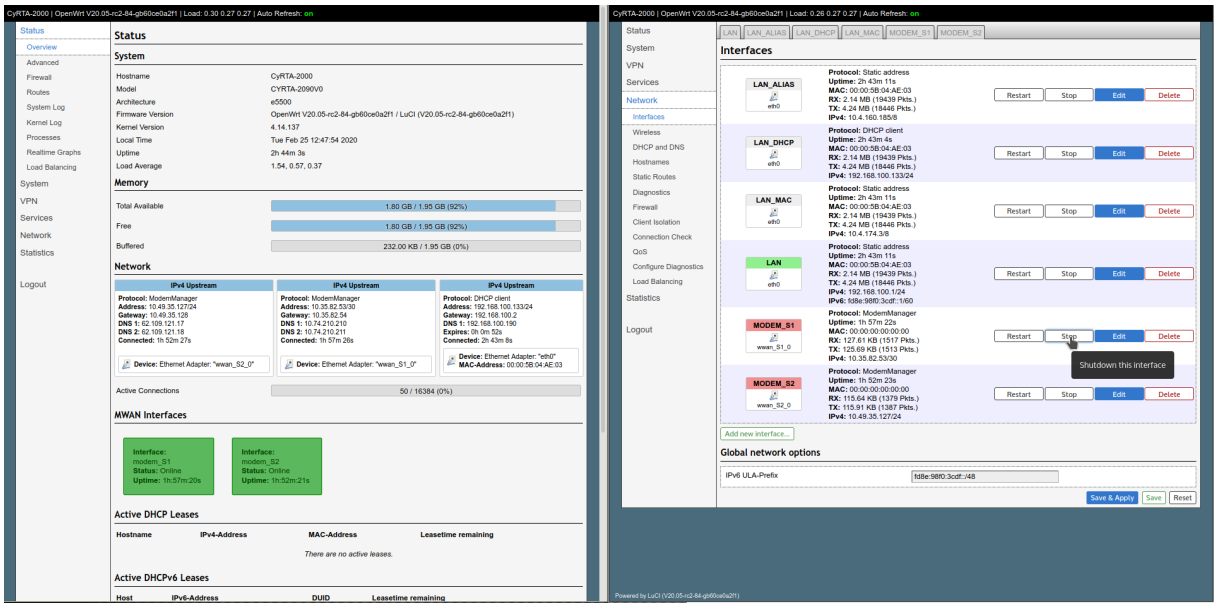
- bietet einen Lastausgleich für ausgehenden WAN-Verkehr über mehrere WAN- Schnittstellen auf der Grundlage einer numerischen Gewichtszuweisung
- überwacht WAN-Verbindungen durch wiederholte Ping-Tests (ping | arping | httping) und leitet ausgehenden Datenverkehr automatisch auf eine andere WAN-Schnittstelle um, wenn die erste WAN-Schnittstelle die Verbindung verliert
- bietet spezifische Regeln für ausgehenden Verkehr, um festzulegen, welche ausgehenden Verbindungen welche WAN-Schnittstelle verwenden sollen

6.1.3.2 MWAN-Test

6.1.3.2.1 Gateway

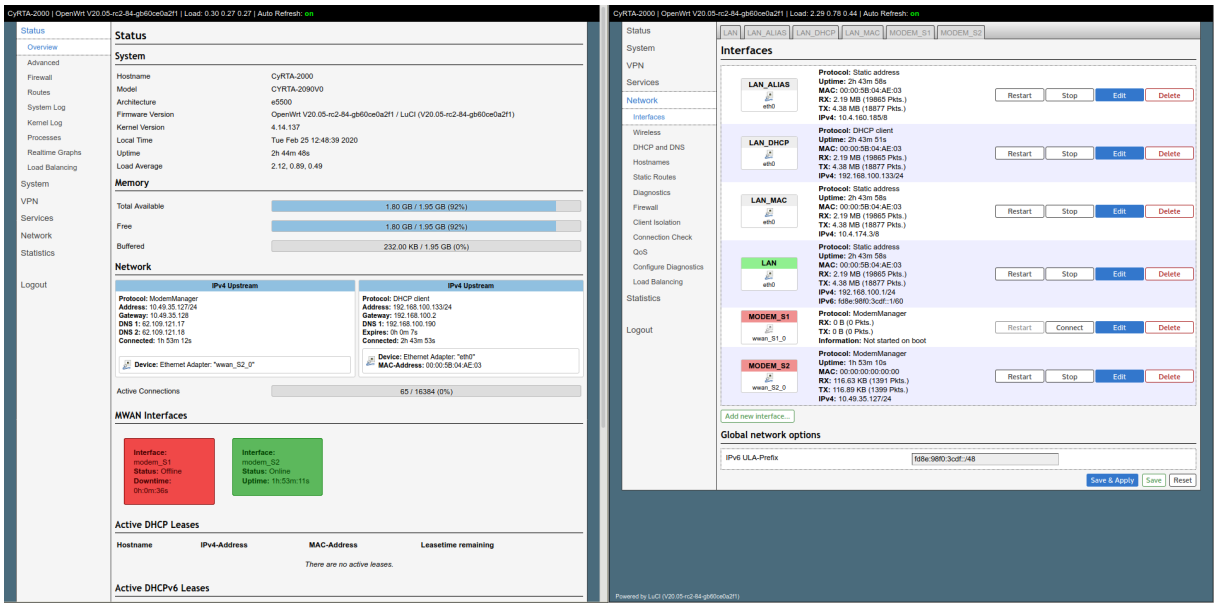
Nach Abschluss der Modem-Konfiguration sind die Modem-Schnittstellen und die Verfolgung per Ping aktiv. Um den Hotplug-MWAN-Mechanismus zu überprüfen, öffnen Sie eine zweite Weboberfläche zu der CyBox AP 2 und gehen Sie zu `Network` → `Interfaces`.

In diesem Beispiel hat `MODEM_S1` die niedrigste Metrik und ist das erste Standard-Gateway. Der Test wird mit der Aktion *Stop* auf der Schnittstelle `MODEM_S1` gestartet.



MWAN-Test zum Stoppen eines Modems

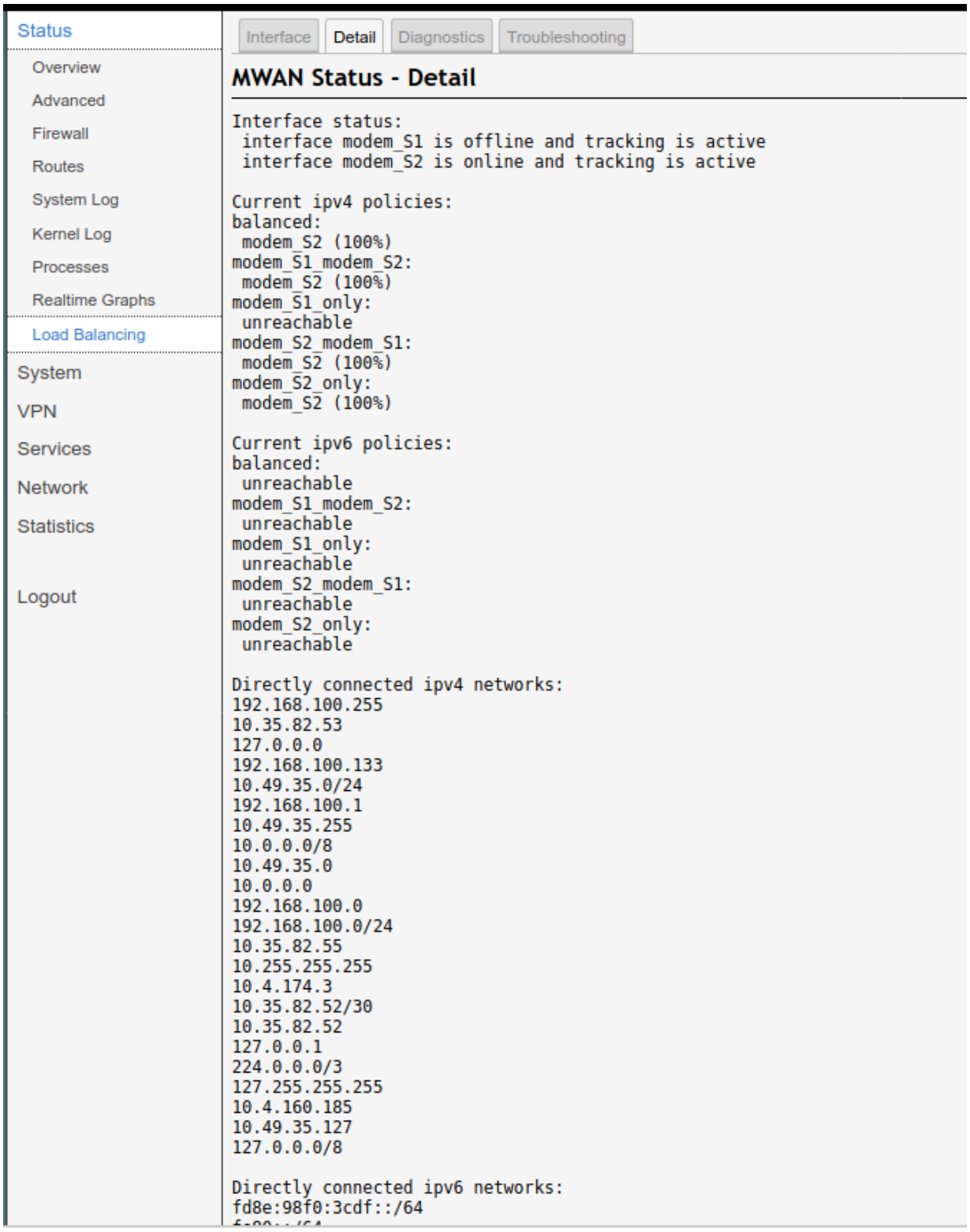
Da die Schnittstelle nicht verfügbar ist, wurde der gesamte Datenverkehr gestoppt und das Standard-Gateway wechselt zu Modem1.



MWAN-Test

6.1.3.3 MWAN-Status

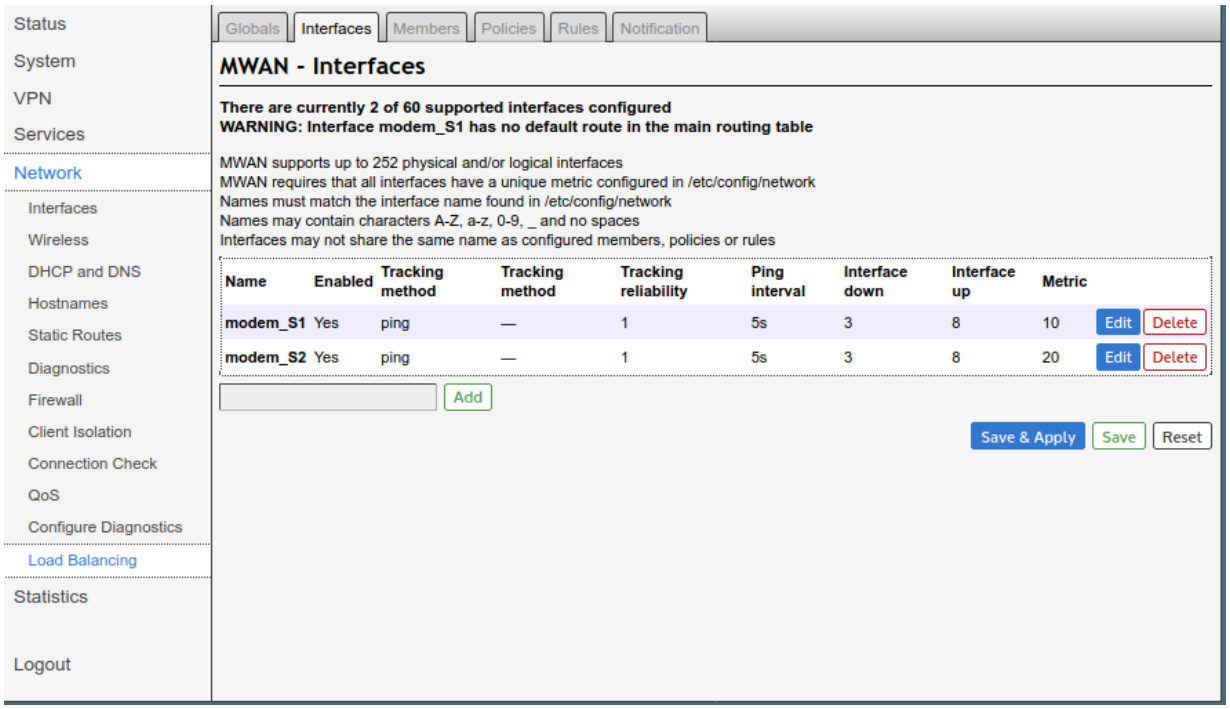
Die detaillierten MultiWan-Statusinformationen finden Sie unter Status → Load Balancing → Detail.



MWAN-Detail-Statusseite

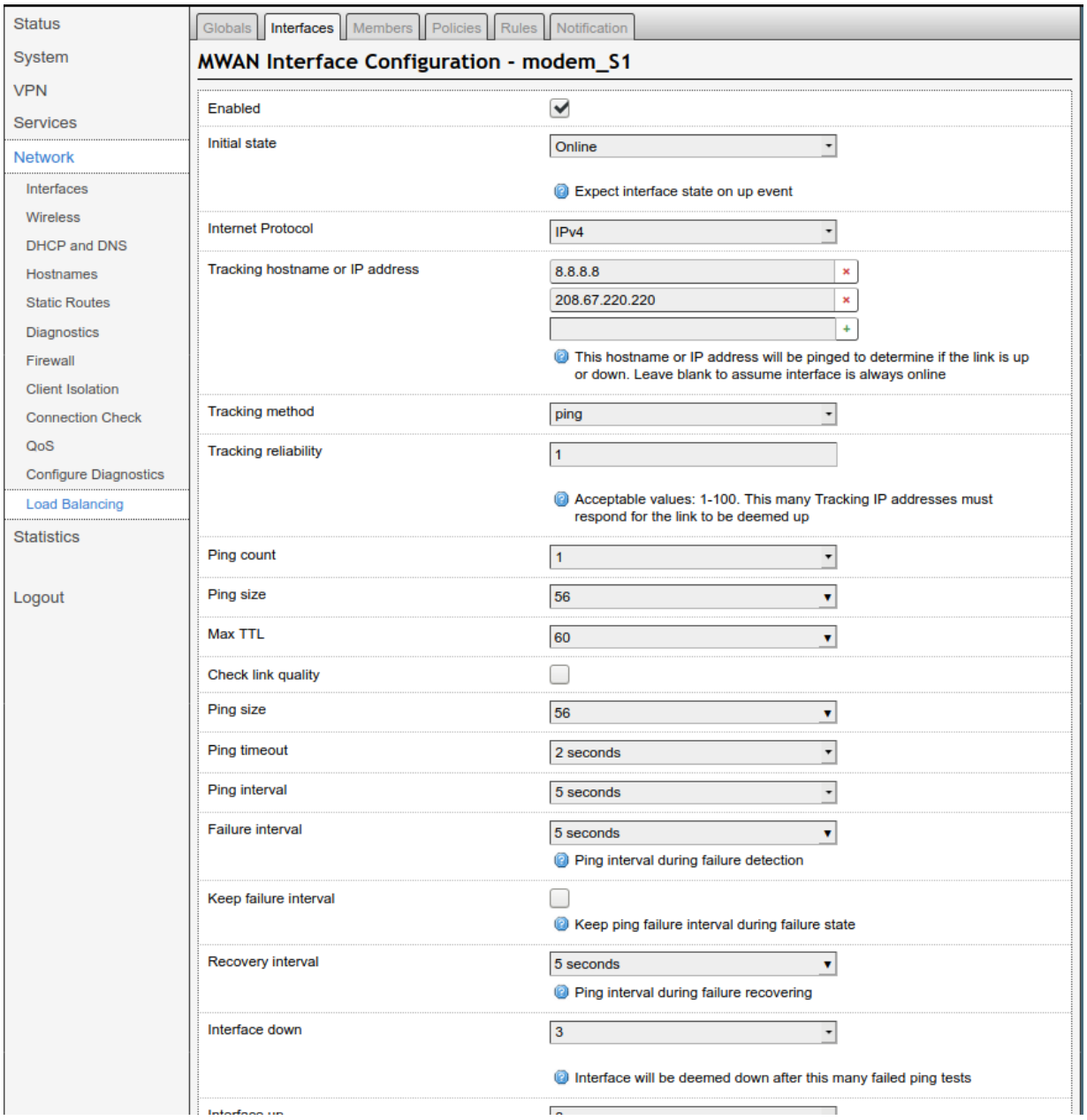
6.1.3.4 Konfiguration der MWAN-Modem-Schnittstelle

Die MWAN-Schnittstellenkonfiguration verfügt über eine Standardeinstellung für jede Modemkarte.



MWAN-Interface-Konfiguration

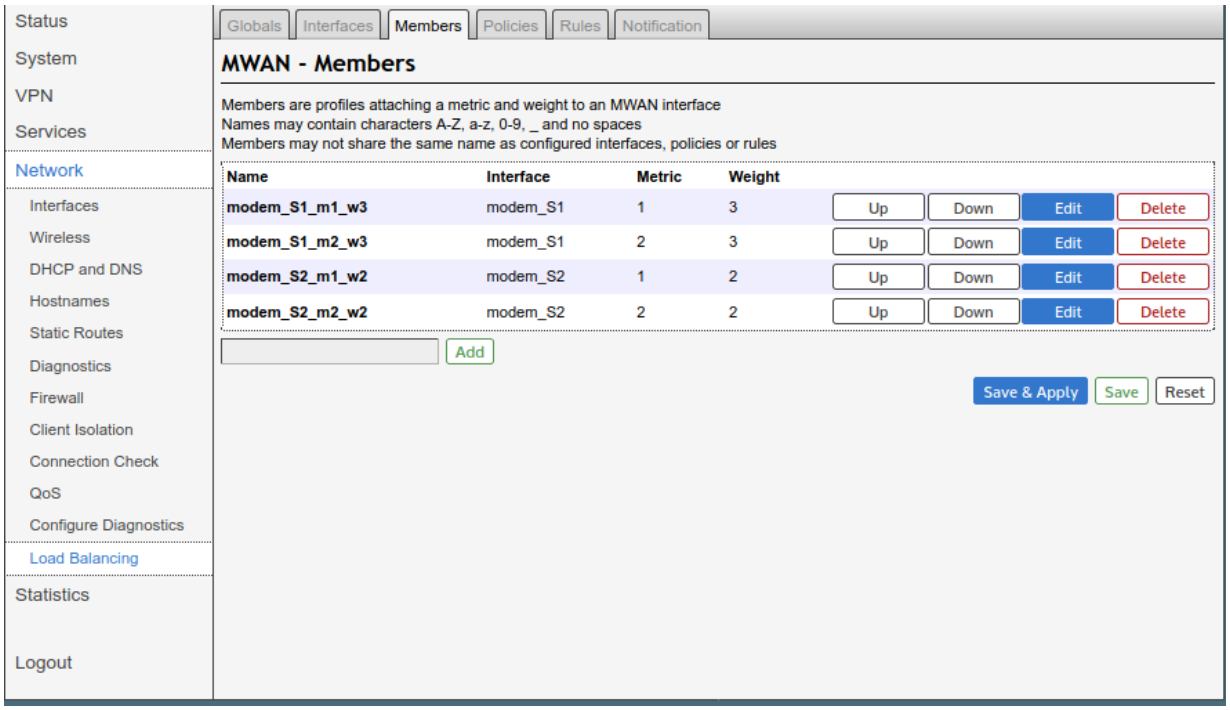
Die Tracking-Parameter können Ziel-Host-IPs, Ping-Intervalle und Timeout verarbeiten.



Tracking-Parameter

6.1.3.5 MWAN-Teilnehmer Konfiguration

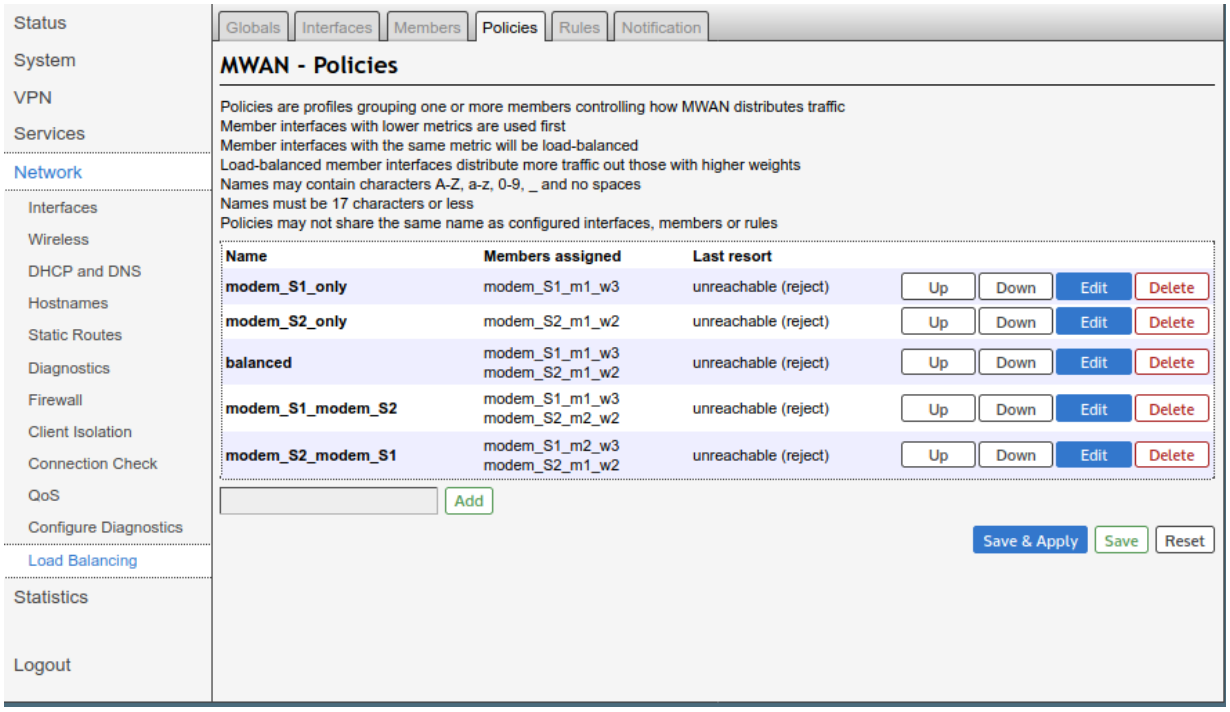
Teilnehmer sind Profile, die einer MWAN-Schnittstelle eine Metrik und ein Gewicht zuordnen. Namen dürfen die Zeichen A-Z, a-z, 0-9, _ und keine Leerzeichen enthalten. Teilnehmer dürfen nicht denselben Namen wie konfigurierte Schnittstellen, Richtlinien oder Regeln enthalten.



MWAN-Teilnehmer

6.1.3.6 MWAN-Richtlinien Konfiguration

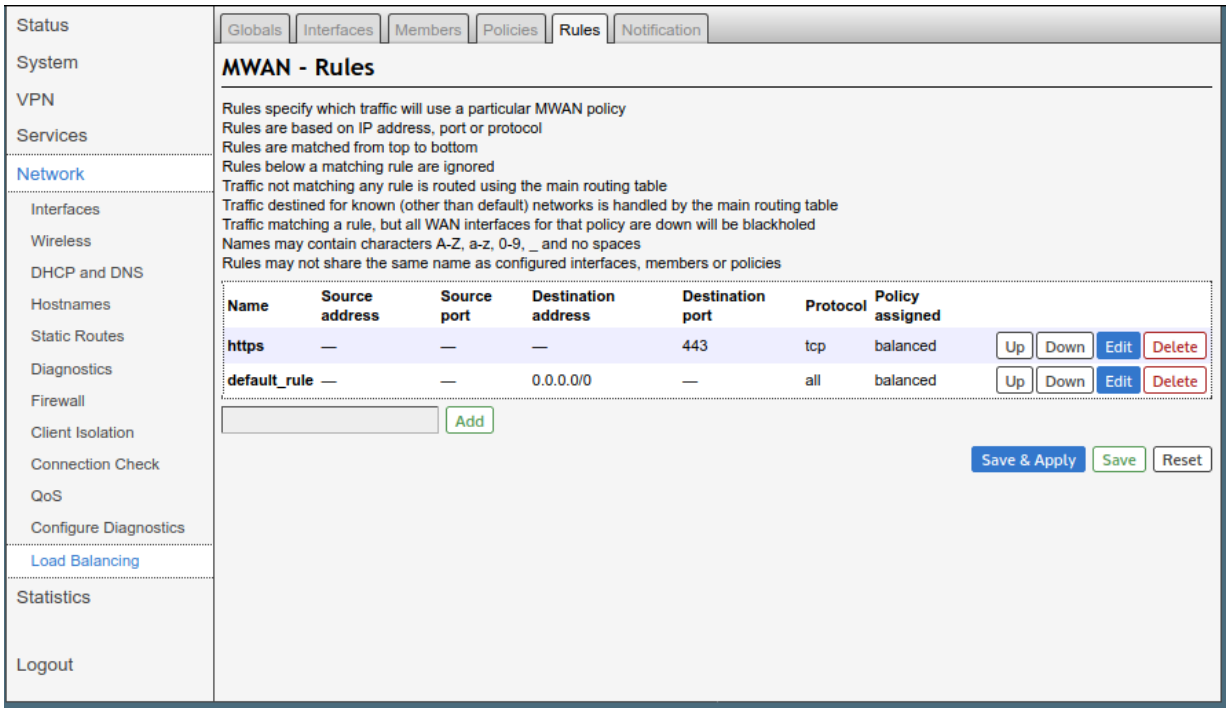
Richtlinien sind Profile, die ein oder mehrere Teilnehmer gruppieren und steuern, wie das MWAN den Datenverkehr verteilt. Teilnehmerschnittstellen mit niedrigeren Metriken werden zuerst verwendet. Schnittstellen mit der gleichen Metrik verwenden den Lastausgleich. Teilnehmerschnittstellen mit Lastausgleich verteilen mehr Verkehr über die Schnittstellen mit höherer Gewichtung.



Seite der MWAN-Richtlinien

6.1.3.7 Konfiguration der MWAN-Regeln

Regeln legen fest, welcher Datenverkehr eine bestimmte MWAN-Richtlinie auf der Basis von IP-Adresse, Port oder Protokoll verwenden soll. Regeln werden von oben nach unten abgeglichen. Regeln unterhalb einer passenden Regel werden ignoriert. Verkehr, der keiner Regel entspricht, wird über die Haupt-Routing-Tabelle weitergeleitet. Datenverkehr, der für bekannte (andere als Standard-) Netzwerke bestimmt ist, wird über die Haupt-Routing-Tabelle geleitet. Datenverkehr, der einer Regel entspricht, bei dem aber alle WAN-Schnittstellen für diese Richtlinie deaktiviert sind, wird gesperrt.



Seite mit MWAN-Regeln

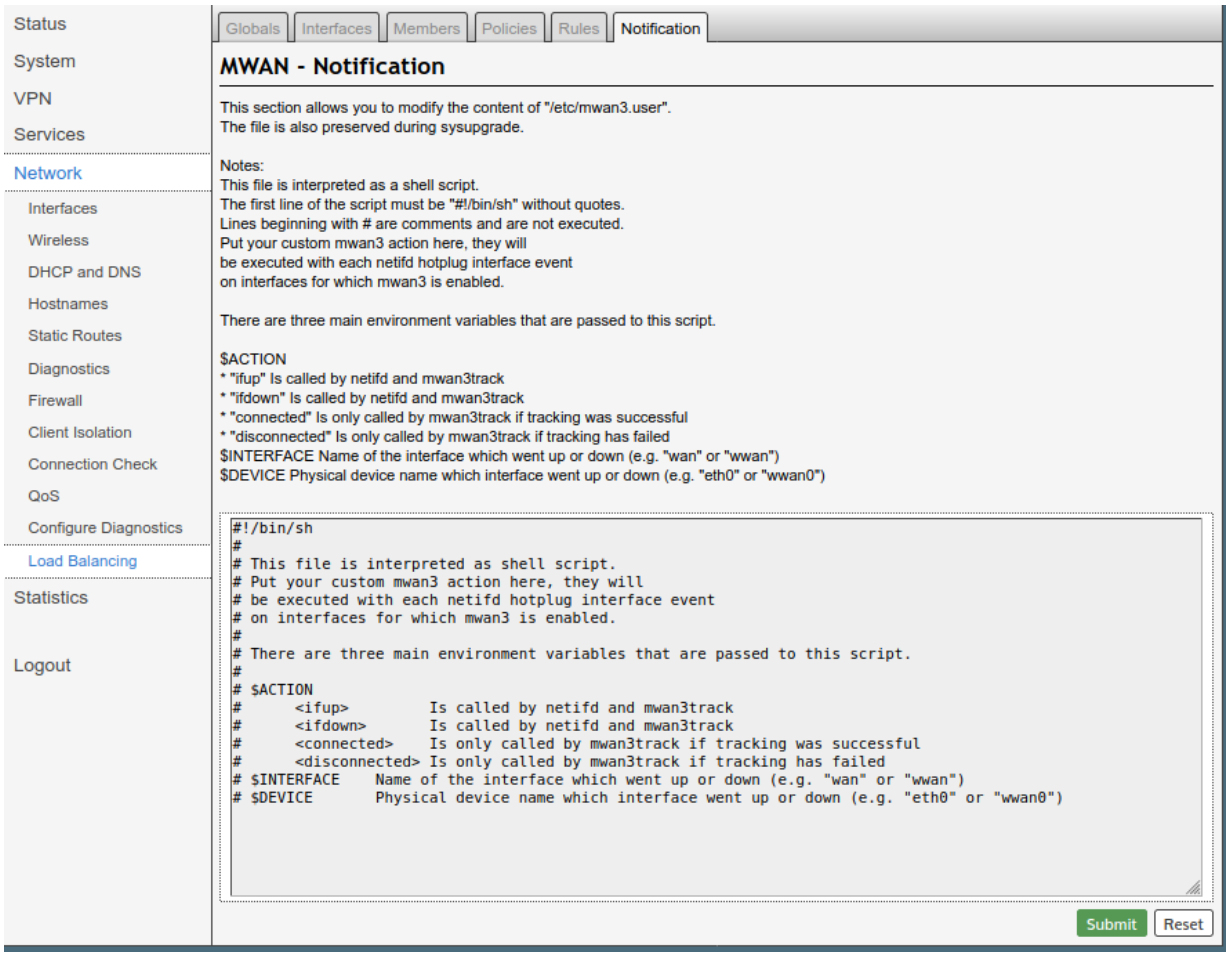
6.1.3.8 Konfiguration der MWAN-Benachrichtigung

In der erweiterten Konfiguration können Sie eine benutzerdefinierte spezifische Aktion für MWAN3-Hotplug-Ereignisse auf Schnittstellen hinzufügen, für die MWAN3 aktiviert ist.

In diesem Abschnitt können Sie den Inhalt von „/etc/mwan3.user“ ändern. Die Datei bleibt auch während des Sysupgrads erhalten.

Hinweise:

- Diese Datei wird als Shell-Skript interpretiert.
- Die erste Zeile des Skripts muss „#!/bin/sh“ ohne Anführungszeichen enhalten.
- Zeilen, die mit # beginnen, sind Kommentare und werden nicht ausgeführt.
- Es gibt drei Hauptumgebungsvariablen, die an dieses Skript übergeben werden:
- $ACTION Entweder „ifup“ oder „ifdown“
- $INTERFACE Name der Schnittstelle, die hoch- oder heruntergefahren wurde (z. B. „wan“ oder „wwan“)
- $DEVICE Physikalischer Gerätename, welche Schnittstelle hoch- oder heruntergefahren ist (z. B. „eth0“ oder „wwan0“)



Konfiguration der MWAN-Benachrichtigung

6.1.4 LACP / Bonding

Bessere Gesamtbandbreite und ausfallsichere Verbindungen durch Verwendung des Link Aggregation Control Protocol (LACP).

Die Kombination mehrerer Gigabit-Ethernet-Schnittstellen zu einer einzigen logischen Bonding-Schnittstelle führt zu einer erhöhten Gesamtbandbreite zwischen den angeschlossenen Geräten.

Detaillierte Informationen zu den Parametern der Bonding-Schnittstelle finden Sie unter Linux Kernel documentation.

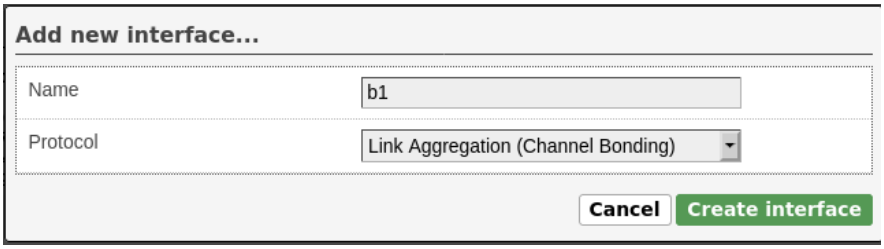
6.1.4.1 Beispiel für eine LACP-Konfiguration

Das folgende Beispiel zeigt eine schrittweise Anleitung zur Konfiguration und zum Test von LACP mit zwei Gigabit Ethernet-Geräten.

> **Wichtig**
>
> Bitte verwenden Sie für die Kommunikation mit der Benutzeroberfläche eine andere Schnittstelle als die, die Sie für LACP verwenden möchten.

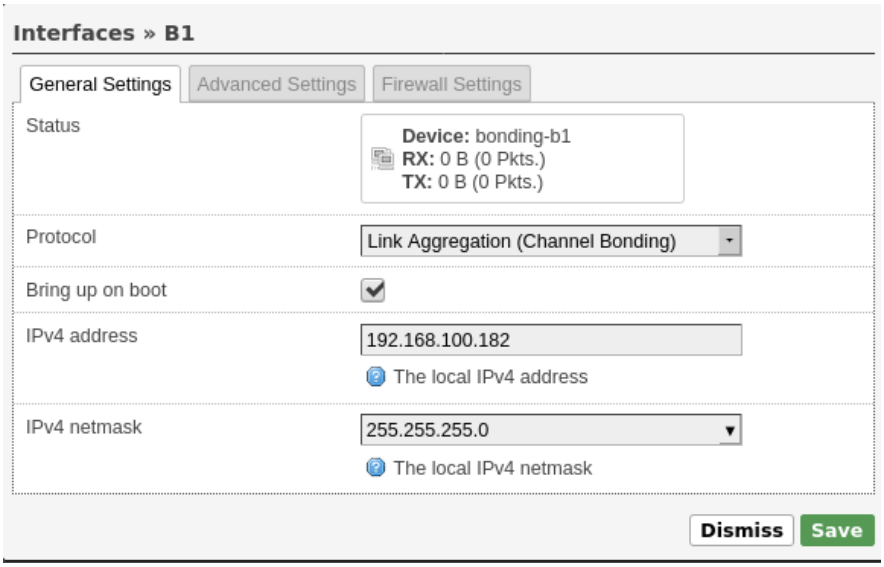
6.1.4.1.1 LACP-Schnittstelle erzeugen

Als erstes sollte eine logische Bonding-Schnittstelle erstellt werden. Dies kann mit Hilfe der UI-Seite (`Network` → `Interfaces` → `Add new interface`) geschehen.



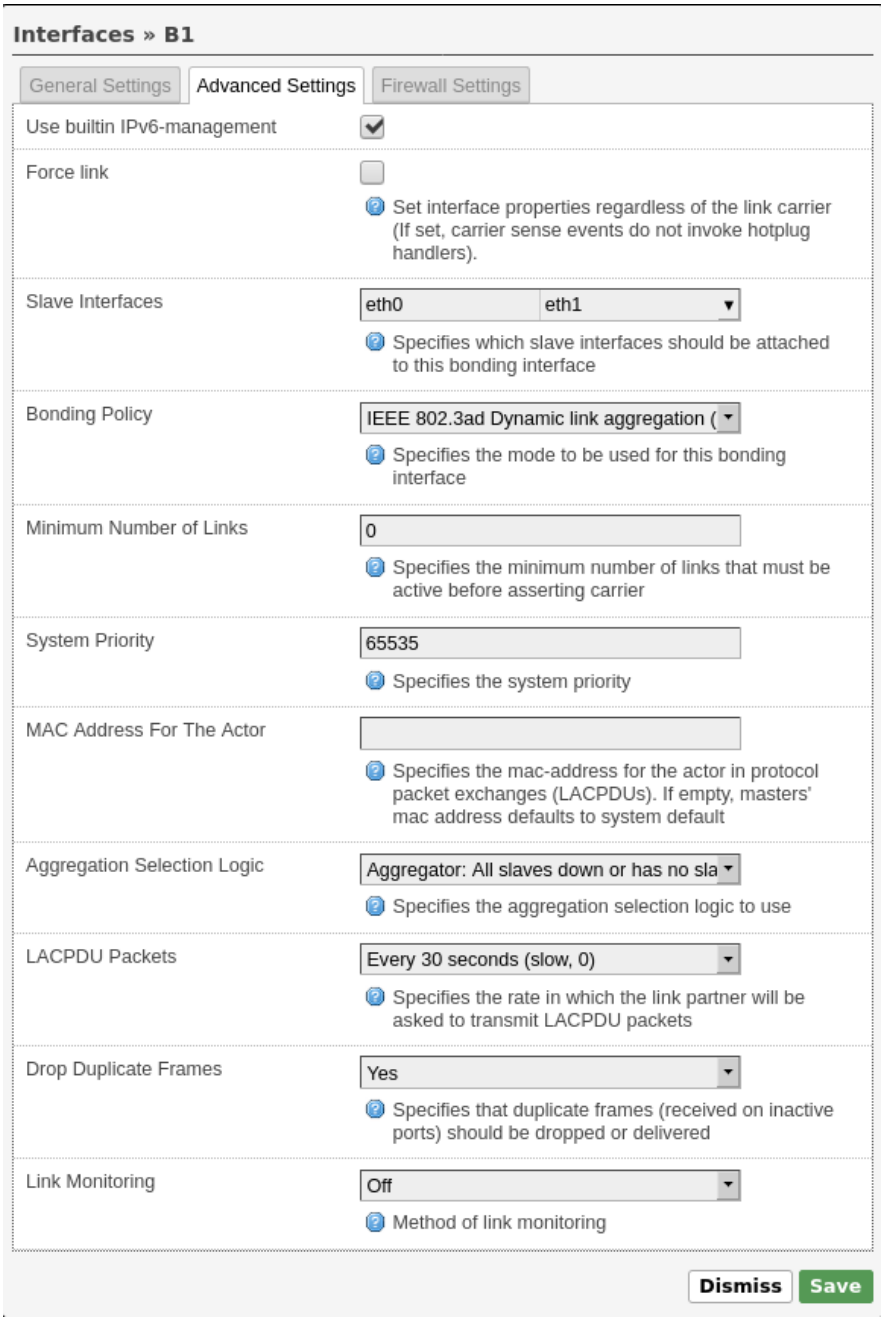
6.1.4.1.2 Einrichtung IP / Netzmaske

Der nächste Schritt ist das Einstellen einer IP-Adresse und einer Netzmaske für die neu erstellte Bonding-Schnittstelle (siehe Registerkarte -> General Settings).



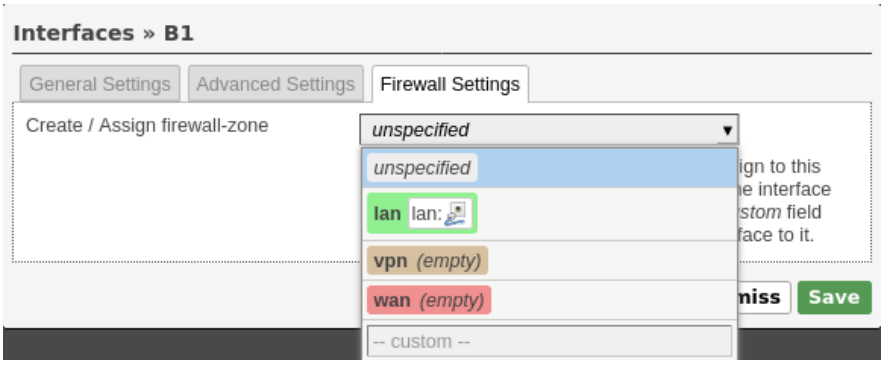
6.1.4.1.3 Bonding Policy einrichten / Slave-Schnittstellen hinzufügen

Slave-Schnittstellen und Bonding-Policy (IEEE 802.3ad = LACP) können über die Registerkarte `Advanced Settings` konfiguriert werden.



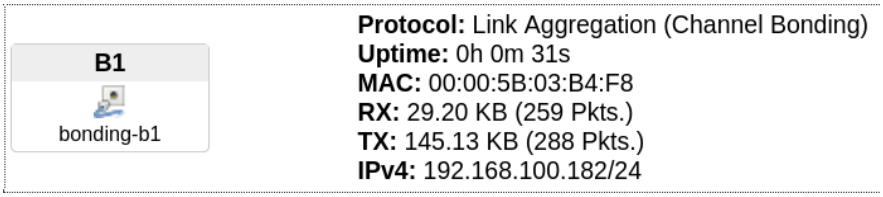
6.1.4.1.4 Einrichten der Firewall

Falls erforderlich, kann die Firewall-Konfiguration über die Registerkarte `Firewall Settings` vorgenommen werden.



6.1.4.1.5 Schnittstellenstatus prüfen

Nach der Anwendung der neuen Konfigurationseinstellungen sollte die Bonding-Schnittstelle `bonding-b1` betriebsbereit sein.



Der Schnittstellenstatus kann auch mit Hilfe der Debug-Konsole überprüft werden.

```
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
    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:~#
```

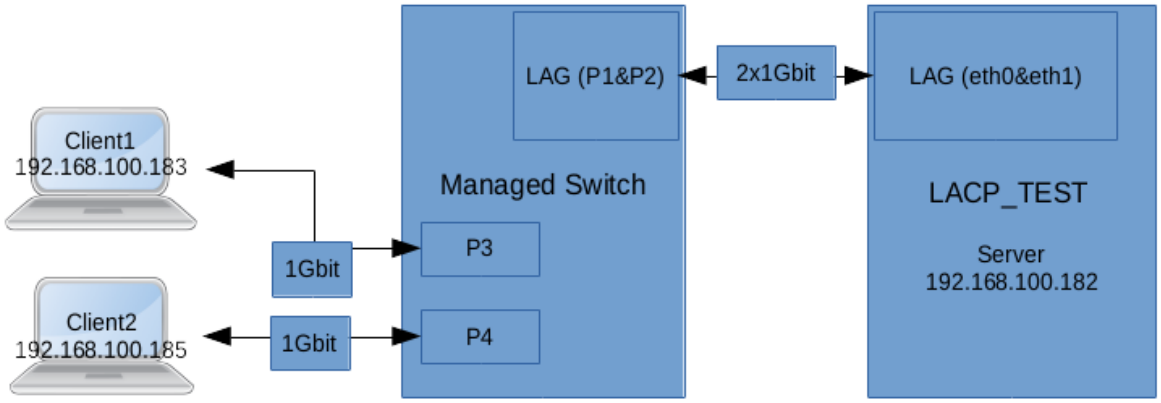
6.1.4.2 Beispiel für einen LACP-Test

Nachdem die Bonding-Schnittstelle konfiguriert und in Betrieb ist, wird zusätzliche Hardware zur Überprüfung der Funktionalität benötigt.

Eines der häufigsten Bonding-Nutzungsszenarien ist die Verbesserung der Bandbreite und der Zuverlässigkeit zwischen Server und Client's.

6.1.4.2.1 Versuchsaufbau

Für ein praktisches Setup werden ein managed Switch mit LACP-Unterstützung, unser zuvor konfiguriertes LACP_TEST-Gerät sowie zwei Client-PCs mit 1 Gigabit-Ethernet-Schnittstelle benötigt.



6.1.4.2.2 Verbesserung der Testbonding-Bandbreite

Ohne die Verwendung der logischen Bonding-Schnittstelle würde die maximal verfügbare Bandbreite zwischen Switch und LACP_TEST-Gerät rein theoretisch 1 Gbit betragen. Die an den Switch angeschlossenen Client-PCs würden sich also diese Bandbreite teilen und jeweils nicht mehr als 500 Mbit erhalten. Da wir zwei 1-Gigabit-Ethernet-Geräte auf eine logische Bonding-Schnittstelle konfiguriert haben, sollte die maximale Bandbreite 2 Gbit betragen. Jeder Client sollte mit dem Server mit einer maximalen Bandbreite von 1000 Mbits kommunizieren können.

In der Praxis kann die theoretisch mögliche Bandbreite nicht erreicht werden! Die maximale Bandbreite wäre ca. 50-60% mehr als ohne Bonding, also nicht 100%!

Als Messwerkzeug wird `iperf` verwendet. Auf dem Gerät LACP_TEST läuft eine iperf-Server-Instanz. Beide Client-PCs kommunizieren gleichzeitig mit der iperf-Server-Instanz auf dem LACP_TEST-Gerät. Während des Tests sehen wir beide Slaves des LACP_TEST Bonding Interfaces laufen. Jeder Client kommuniziert mit der iperf-Instanz des Servers über eine der beiden Slave-Schnittstellen mit einer Bandbreite von etwa 800 Mbits.

6.1.4.2.3 Verbesserung der Zuverlässigkeit des Test-Bondings

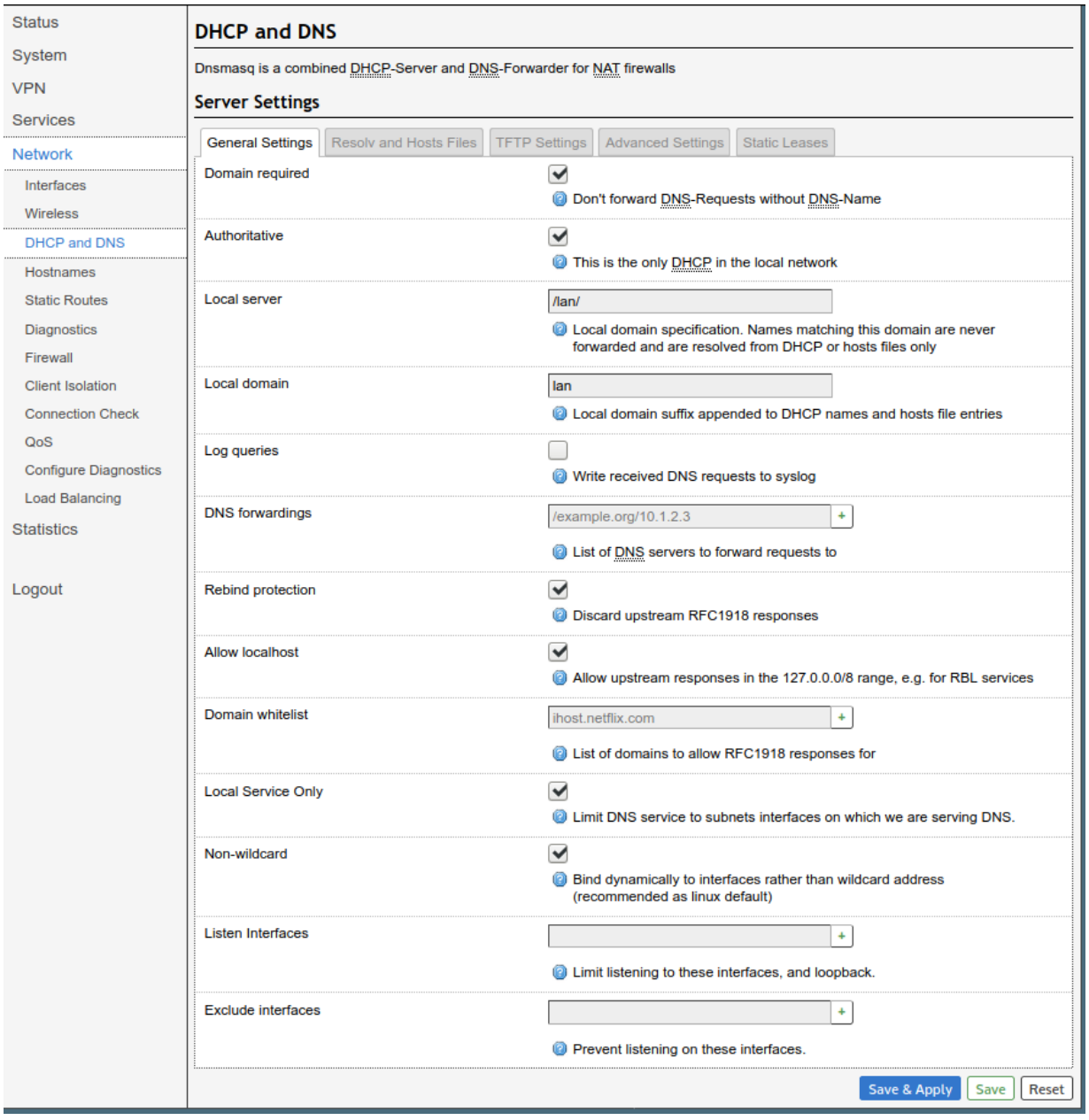
Falls die Switch<->Server-Verbindung ohne LACP läuft, führt jeder Kommunikationsfehler zu einer unterbrochenen Client-Verbindung. Aufgrund der verbesserten Zuverlässigkeit der Bonding-Implementierung funktioniert die Kommunikation zwischen Clients und Server auch, wenn einer der beiden LACP-Slaves ausfällt. Dieses Szenario kann leicht überprüft werden, indem man einen der beiden Bonding-Slaves, z. B. eth0, abklemmt.

6.1.5 Globale DHCP- und DNS-Einstellungen

Vergewissern Sie sich, dass Sie die DHCP- und DNS-Dienste verstehen, bevor Sie irgendwelche Konfigurationen ändern. Unter normalen Umständen sollte die Beibehaltung der Werkseinstellung ausreichend sein.

Die CyBox AP 2 verwendet einen DNS-, TFTP- und DHCP-Server. Er ist dazu gedacht, einen gekoppelten DNS- und DHCP-Dienst für ein LAN bereitzustellen. Dieser Dienst nimmt DNS-Anfragen entgegen und beantwortet sie entweder aus einem kleinen, lokalen Cache oder leitet sie an einen echten, rekursiven DNS-Server weiter. Siehe Kapitel DHCP-Server 6.1.1.1 DHCP-Server pro Interface .

Der DHCP-Server unterstützt statische Adresszuweisungen und mehrere Netzwerke. Er sendet automatisch eine sinnvolle Standardeinstellung von DHCP-Optionen und kann so konfiguriert werden, dass er jeden gewünschte Einstellung von DHCP-Optionen sendet, einschließlich herstellergekapselter Optionen. Er enthält einen sicheren, schreibgeschützten TFTP-Server, der das Booten von DHCP-Hosts per Net/PXE ermöglicht, und unterstützt auch BOOTP.



Bildschirm zur Konfiguration von DHCP und DNS

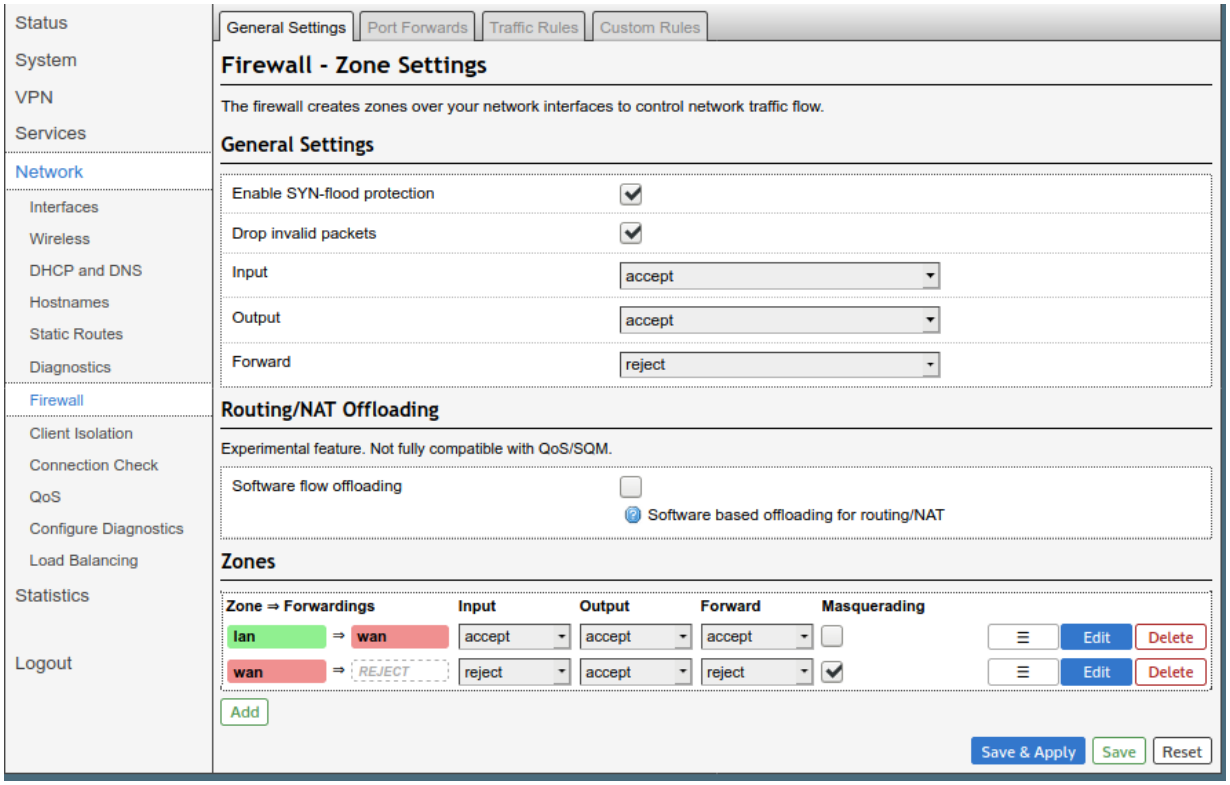
6.1.6 Firewall

Stellen Sie sicher, dass Sie zonenbasierte Firewalls verstehen, bevor Sie die Firewall-Konfigurationen ändern.

Die CyBox AP 2 hat eine eingebaute Stateful-Firewall, die Schnittstellen in Zonen abbildet, die verwendet werden, um Standardregeln für eine bestimmte Schnittstelle, Weiterleitungsregeln zwischen Schnittstellen und zusätzliche Regeln, die nicht von den ersten beiden abgedeckt werden, zu beschreiben.

Die erste Regel, die zutreffend ist, wird ausgeführt und führt oftmals zu einer weiteren Regelkette, bis ein Paket entweder auf ACCEPT oder DROP/REJECT trifft. Ein solches Ergebnis ist endgültig, daher treten die Standardregeln zuletzt in Kraft, und die spezifischste Regel tritt zuerst in Kraft. Zonen werden auch zur Konfiguration von Masquerading, auch bekannt als NAT (network-address-translation), sowie von Portweiterleitungsregeln verwendet, die allgemeiner als Redirects bekannt sind.

Zonen müssen immer auf eine oder mehrere Schnittstellen abgebildet werden, die letztlich auf physische Geräte abgebildet sind; daher können Zonen nicht verwendet werden, um Netzwerke (Subnetze) zu spezifizieren, und die generierten iptables-Regeln arbeiten ausschließlich auf Schnittstellen. Der Unterschied besteht darin, dass Schnittstellen verwendet werden können, um Ziele zu erreichen, die nicht zu ihrem eigenen Subnetz gehören, wenn ihr Subnetz ein anderes Gateway enthält. Normalerweise erfolgt die Weiterleitung jedoch zwischen LAN- und WAN-Schnittstellen, wobei der Router als „Edge“-Gateway zum Internet dient. Die Standardkonfiguration der Firewall sieht eine algemein übliche Einrichtung vor.



Bildschirm zur Einstellung der Firewall-Zone

6.1.7 OpenVPN

Ab der Firmware-Version 3.2 ist die Open-Source-VPN-Lösung enthalten. Die Firmware vor Version 4.0 unterstützt kein Web-Frontend für die OpenVPN-Konfiguration.

Das OpenVPN-Programm verfügt über viele Parameter, um eine Verbindung aufzubauen. In diesem Kapitel wird eine grundlegende Client-OpenVPN-Tunnelkonfiguration beschrieben. Im nächsten Beispiel wird die VPN-Tunnelverbindung über eine bereits laufende LTE-Schnittstelle hergestellt, die das Internet-Gateway bereitstellt.

6.1.7.1 Generierung von Konfigurationsdateien unter Windows

OpenVPN für Windows kann eine OpenVPN-GUI verwenden, die die Verwaltung von OpenVPN-Verbindungen über ein System-Tray-Applet ermöglicht. Es kann verwendet werden, um eine vollständige Client-Konfiguration (Zip-Datei) einschließlich der .ovpn-Konfigurationsdatei zu erzeugen.

6.1.7.2 Einrichtung der VPN-Schnittstelle - 3 Methoden

Der Aufbau der VPN-Verbindung kann mit den drei folgenden Methoden erreicht werden.

6.1.7.2.1 Gebrauchsfertige Konfiguration mit SCP kopieren

Dies ist der einfachste Weg, eine VPN-Verbindung zu konfigurieren. Es wird vorausgesetzt, dass die Serverseite über eine konfigurierte Netzwerkumgebung verfügt. Der Server-Administrator sollte ein gültiges

Client-Konfigurationspaket erstellen, das Zertifikate, Client-Schlüssel und vorzugsweise eine Konfigurationsdatei myclient.ovpn enthält. Die VPN-Verbindung wird auf dieser Konfigurationsdatei (myclient.ovpn) aufgebaut. Dieses Beispiel verwendet vier Dateien, die statisch auf der CyBox AP 2 gespeichert sein müssen, damit das Programm openvpn eine Verbindung ohne Benutzerinteraktion aufbauen kann. Wenn die Option ‚auth-user-pass' ohne Parameter an openvpn übergeben wird, wird der Verbindungsaufbau unterbrochen und nach einem Benutzernamen und Passwort gefragt. Damit dies automatisch abläuft, muss eine zweizeilige Datei mit Benutzernamen (in der ersten Zeile) und Passwort (in der zweiten Zeile) angegeben werden. Alle vier Dateien, die ‚auth_user_pass', die ‚pfelt1-udp-vpnuser_fg.p12' , die Benutzer-Schlüsseldatei ‚pfelt1-udp-vpnuser_fg-tls.key' und die Konfigurationsdatei ‚myclient.ovpn' müssen vom Host-System über den Befehl ‚scp' in den permanenten Speicher im Verzeichnis ‚/etc/openvpn/' kopiert werden. Stellen Sie sicher, dass alle Dateien in ‚/etc/openvpn' die Dateiberechtigung 600 haben (cd /etc/openvpn; chmod 600 *).

Die ‚myclient.ovpn'-Konfiguration ist:

```
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
```

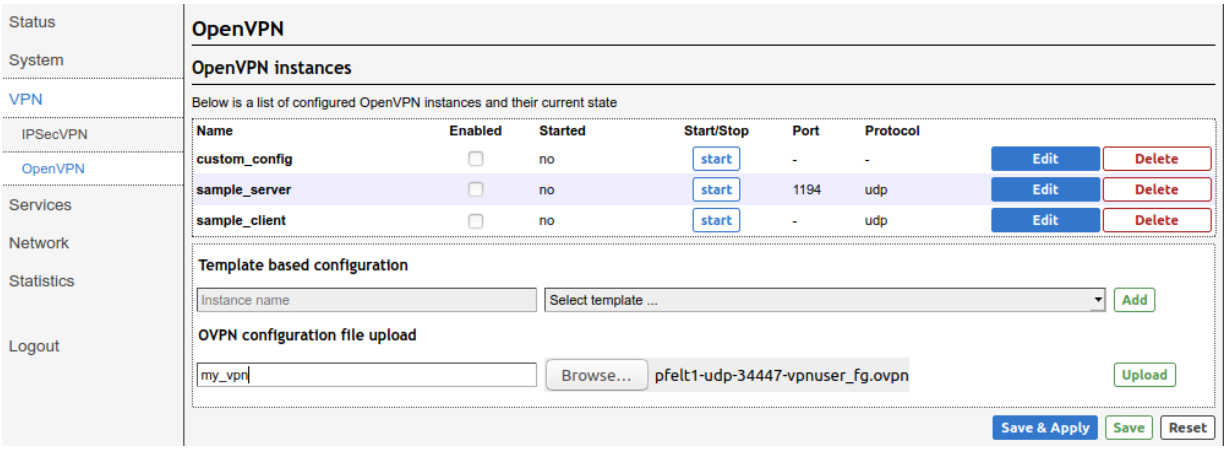
6.1.7.2.2 Hochladen von Konfiguration, Zertifikaten und Schlüsseldateien mit Web-Interface

Die zweite Methode ist ganz ähnlich wie die erste. Es wird eine modifizierte Datei „myclient.ovpn" verwendet. Der Unterschied besteht darin, dass das Zertifikat, die Schlüsseldateien und die Passwortdateien über die Weboberfläche hochgeladen werden. Das Standard-Upload-Verzeichnis der Weboberfläche ist /etc/luci-uploads/ und die hochgeladene Datei wird mit dem Diensttyp und dem Schnittstellennamen versehen, z. B.:

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

Fügen Sie in einem ersten Schritt Ihre neue VPN-Konfiguration über eine Vordefinition hinzu.

1. Neue VPN-Konfiguration unter Verwendung einer Vordefinition:



Bearbeiten Sie Ihre config.ovpn-Datei und stellen Sie sicher, dass alle Zertifikate, Schlüsseldateien, Benutzername-Pass-Dateien den richtigen Pfad einschließlich Ihres Konfigurationsnamens haben, hier ‚my_vpn'.

Die vorbereitete ‚myclient.ovpn'-Konfiguration sieht so aus und ist bereit zum Hochladen:

(hochgeladen nach /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
```

6.1.7.2.3 Manuelle Konfiguration mit Webinterface

Die dritte Methode verwendet keine vorkonfigurierte .ovpn-Datei. Sie müssen jeden einzelnen Parameter in der Weboberfläche eingeben. Beim Starten des Dienstes werden alle angegebenen Parameter an das Programm ‚openvpn' übergeben. Diese Methode kann für ein schnelles Umschalten der Parameter für Server und Client nützlich sein.

6.1.7.3 VPN-Host-Konfiguration (auf Konsole)

Nachdem die Konfiguration des VPN-Client-Teils abgeschlossen ist, ist es an der Zeit, den Rest des Systems zu konfigurieren und eine erste Verbindung zu starten. Diese Konfiguration kann an der Konsole (über SSH) mit ‚uci'-Befehlen vorgenommen werden.

Die Ausführung des Programms openvpn auf dem CyBox AP 2 wird mit dem Skript ‚/etc/init.d/openvpn' verwaltet.

Die folgende Konfiguration wird an der Eingabeaufforderung vorgenommen:

Erstellen Sie die VPN-Schnittstelle (wenn keine Server-Bridge läuft):

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

Eingehenden VPN-Verkehr zulassen:

```
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>`__
```

OpenVPN-Tunnelnutzung zulassen: (nicht erforderlich bei Überbrückung mit 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
uci set firewall.@forwarding[-1].src='lan'
uci set firewall.@forwarding[-1].dest='vpn'
```

Speichern Sie die Änderungen:

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

Aktivieren Sie das Startflag und richten Sie die Konfigurationsdatei ein:

```
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
```

Machen Sie schließlich einen ersten Test und starten Sie die openvpn-Verbindung manuell:

```
/etc/init.d/openvpn start
```

Verwenden Sie den Befehl ‚logread', um den Fortschritt der Verbindung zu beobachten.

```
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
```

6.1.8 ICCP

Das **I**nter **C**arriage **C**onnection **P**rotocol ist ein von ELTEC entwickelter Bridging-Algorithmus zum automatischen Aufbau und zur Wartung eines Wireless-LAN-Backbone für Züge. Es kann in Retrofit-Applikationen eingesetzt werden, bei denen es zu teuer ist, Backbone-Ethernet-Kabel im gesamten Zug zu installieren. Die Herausforderung besteht darin, Verbindungen in einer instabilen Umgebung aufzubauen und aufrechtzuerhalten, die Störungen ausgesetzt ist, wie z.B. Zugumstellungen, Verbindungsverluste oder andere Züge auf Nachbargleisen.

Die Hauptmerkmale von ICCP sind:

- Nutzung von RSSI zur Ermittlung des besten Koppelungspartners in Reichweite
- Verwendung des WDS-Modus (Wireless Distribution System) für AP_Master-Client connection
- Unterstützung aller Verschlüsselungsmodi (WPA2-PSK, etc.)
- Einmalige Konfiguration
- Unbeaufsichtigter Kopplungs-/Entkopplungsprozess, Wiederherstellung von zuvor hergestellten Verbindungen nach Stromausfall
- Freie Kanalwahl in 2,4 GHz mit allen HT-Modes oder 5 GHz mit HT-Modes (20/40/80)

6.1.8.1 Kopplungskonzept

Das Kopplungskonzept folgt verschiedenen Zuständen, in denen der Access Point versucht, den besten Partner für die Kommunikation zu ermitteln, eine Verbindung aufzubauen und diese aufrechtzuerhalten. Die folgende Tabelle gibt einen Überblick über die Zustände.

ICCP-Kopplungszustände:

Status	Beschreibung

IDLE	Das Funkmodul ist aktiviert. Der Standardmodus ist AP mit gesendeter SSID und eigener Seriennummer, die in der SSID codiert ist. Der WLAN-Modus ist als „Access Point (WDS)“ Master mit einer achtstelligen SSID gesendet und eigener Seriennummer kodiert in die SSID konfiguriert. Der LAN-Port ist für Bridging konfiguriert und das Spanning Tree Protocol ist aktiviert.
BIND	WLAN ist aktiviert und das Gerät sucht nach der qualifizierten Gegenstelle mit der besten Signalstärke. Die Suche wird mehrfach wiederholt, um sicherzustellen, dass eine stabile Situation angetroffen wird. Um sich als bester Nachbar zu qualifizieren, ist eine minimale Signalqualität erforderlich. Die ID (fremde Seriennummer) des gefundenen besten Nachbarn wird an den nächsten Zustand CONNECT weitergegeben.
CONNECT	Die eigene ID und die ID des besten gefundenen Nachbarn werden in die neue eigene SSID kodiert; das Gerät wartet auf einen SSID-Broadcast des Nachbargerätes mit der gleichen Kombination der IDs. Dieser Zustand hat ein Zeitlimit, um die Verbindung aufzubauen. Wird es überschritten, fällt der Zustand auf BIND zurück. Der erwartete Client-Partner kann das Zeitlimit für den Master verlängern, um eine gemeinsame SSID zu setzen, und wechselt in den Zustand ESTABLISHED, sobald die SSID die Markierung „EST“ enthält.
ESTABLISHED	Beide Geräte gehen in eine neue Konfiguration über: Das Gerät mit der größeren ID wird „Master“ das andere wird „Client“. Die im vorherigen Zustand ausgehandelte SSID wird ausgeblendet, wenn der Master die Client-MAC erkennt. Der WLAN-Zugangsschlüssel wird aus den IDs abgeleitet.
DROPPED	Verbindung durch Funkstörung oder Zugumbau verloren. Das Gerät versucht für eine vorkonfigurierbare Zeit, die letzte bekannte Verbindung wiederherzustellen.

6.1.8.2 SSID-Nutzung

Das Kopplungsverfahren nutzt die Tatsache aus, dass SSIDs alphanumerische Zeichen enthalten und sie gesendet werden können. Somit kann eine SSID verwendet werden, um für die Kopplung nützliche Informationen zu übertragen und einen Dialog zum Verbindungsaufbau einzugeben. Die Access Points verwenden ihre Seriennummer - eine achtstellige Zahl - um sich zu identifizieren. Zusätzlich kann die SSID Statusinformationen enthalten, damit der potenzielle Kommunikationspartner den Fortschritt der Verhandlung verfolgen kann. In der aktuellen Implementierung werden diese zusätzlichen Zustandsinformationen jedoch nicht verwendet. Die SSIDs beginnen mit einer bekannten Buchstabenfolge („CyAP“), die es ermöglicht, Funkaktivitäten von Access Points anderer Netze herauszufiltern. Ab der Firmware-Version 4.0 ist dieses Start-Tag „CyAP“ veränderbar, muss aber seine Länge von vier Zeichen beibehalten.

Die folgende Tabelle gibt einen Überblick über die verschiedenen Zustände der verwendeten SSIDs.

Verwendete ICCP-SSIDs:

SSID	Beschreibung
CyAPi_oooooooo	SSID wird im BIND-Status gesendet. Die Zeichen ooooo werden durch die eigene Seriennummer des AP ersetzt. Der Buchstabe ‚i‘ repräsentiert den Index des WLAN-Moduls.
CyAPi_oooooooo_ nnnnnnnn	SSID wird im CONNECT-Status gesendet. Die Zeichen ooooo werden durch die eigene Seriennummer des AP ersetzt, die Zeichen nnnnn werden durch die Seriennummer des AP ersetzt, die während des Suchstatus als bester Nachbar erkannt wurde.
CyAPi_oooooooo_ nnnnnnnn	SSID wird zu Beginn des Status ESTABLISHED gesendet. Immer noch das gleiche wie in CONNECT, jedoch nur für einige Sekunden, bis der Master die MAC-Verbindung erkennt.

CyAPi_oooooooo_nnnnnnnn_ESTp	Private SSID (nicht gesendet), die während des Status ESTABLISHED verwendet wird. Die Codierung ist identisch mit der CONNECT SSID. Der Buchstabe ‚p' repräsentiert den Index des Partner-WLAN-Moduls.
CyAPi_oooooooo_nnnnnnnn_<custom-ssid/network>	Nur VLAN-Modus. Private SSID (nicht gesendet), die während des Status ESTABLISHED verwendet wird. Die Codierung ist identisch mit der CONNECT SSID.

6.1.8.3 WLAN-Verschlüsselung

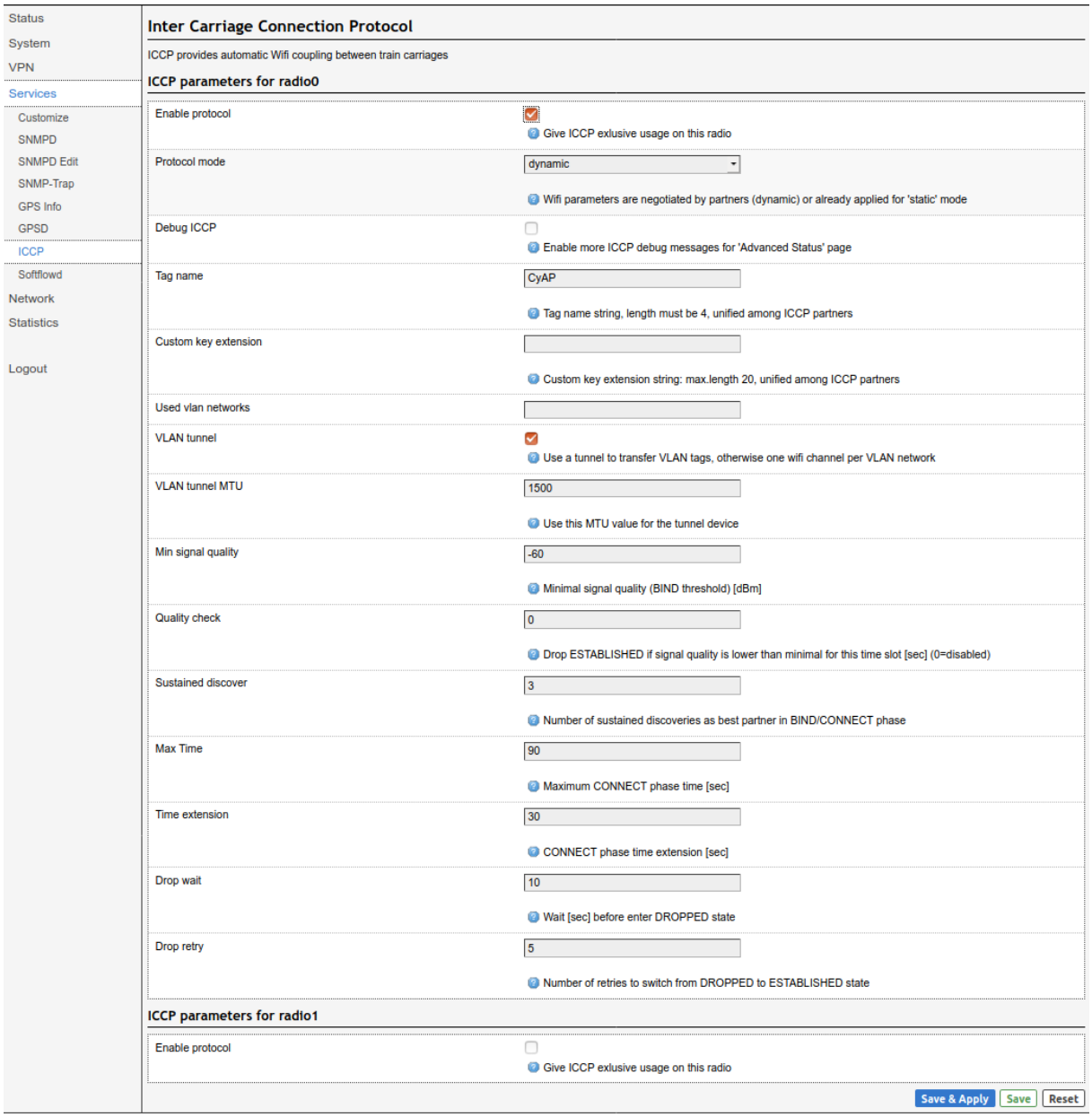
Für die Kommunikation zwischen den Waggons muss ein geeigneter Verschlüsselungmodus aktiviert werden. Zur Authentifizierung müssen individuelle Zugriffsschlüssel (PSK) zwischen den Peers festgelegt werden. Der Schlüssel wird aus der SSID mittels eines Hash-Algorithmus generiert, der beiden Access Points bekannt ist. Im BIND- und CONNECT-Zustand ist der WLAN-Modus auf „Access Point (WDS)" (Wireless Distribution System) eingestellt, wobei ein achtstelliger Zufallsschlüssel zur Verschlüsselung verwendet wird.

6.1.8.4 Konfigurierbare Parameter

Bevor Sie die ICCP-Parameter konfigurieren, stellen Sie sicher, dass die folgenden Aktionen durchgeführt wurden:

- Löschen Sie alle nicht benötigten Schnittstellen mit der Webinterface-Registerkarte Network → Interfaces (z.B. *lan_alias*)
- Konfigurieren Sie Ihre ICCP-Management-Schnittstelle wie gewünscht in `Network` → Interfaces (z. B. konfigurieren Sie die *lan*-Schnittstelle als eine Bridge aus eth0, wlan0 und wlan1, dann setzen Sie die IP-Adresse auf 192.168.100.2)
- Aktivieren Sie in `Network` → WiFi das WLAN-Radio, das Sie für ICCP verwenden möchten (z. B. nur Radio o).

Danach können Sie im Register ‚Services' →'ICCP' mit der Konfiguration von ICCP beginnen. Klicken Sie dann auf 'Save & Apply'.



Bildschirm ICCP-Konfiguration

Hinweis 1: Wenn ICCP ohne VLAN-Verbindungen verwendet wird, muss der ‚dynamic' Modus verwendet werden.

Hinweis 2: ‚Operating frequency parameters' müssen für beide ICCP-Partner identisch sein.

In der folgenden Tabelle 6 sind die Parameter aufgeführt, die das Timing-Verhalten bzw. den Verbindungsablauf beeinflussen.

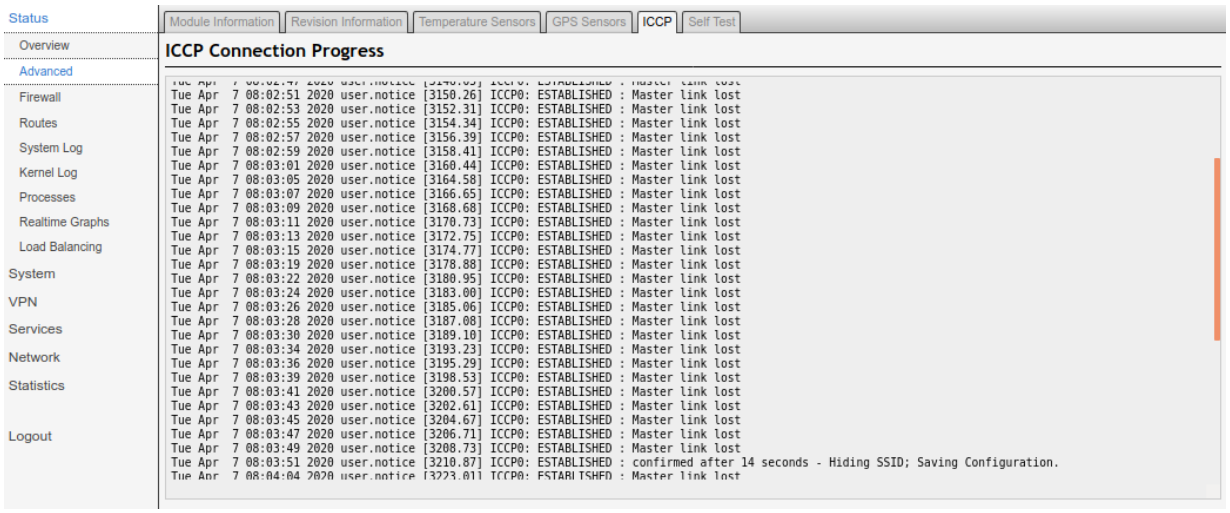
ICCP-Parameter:

Parameter	Beschreibung	Einheit	Bereich	Standardeinstellung

USED_VLAN_NETWORKS	Mit Standard-ICCP: empty - ICCP baut eine Brücke zwischen nativem eth0 und wlan0/1. Mit VLAN ICCP: Liste aller konfigurierten VLAN-Netzwerke/ssid. Namen, bei denen Groß- und Kleinschreibung beachtet wird, für Netzwerkschnittstellen und virtuelle SSIDs sollten zuerst auf den entsprechenden Menüleisten konfiguriert werden.	Comma separated list	custom	empty
CHANNEL_SETTINGS	Vordefinierte Kanaleinstellungen: Stellen Sie sicher, dass alle gewünschten Koppelpartner den gleichen Kanalmodus verwenden.	mode string	predefined or custom	2.4 GHz, CH 11, HT40-
MIN_SIGNAL_QUALITY	Minimale Signalqualität: Partner, die unter diesem Wert liegen, werden ignoriert.	dBm	-100…0	-60
RECOVER	Anzahl der Male, die ein anderer AP in Folge als bester Nachbar erkannt werden muss. Dieser Wert gilt für den Zustand BIND und CONNECT.	times	1…5	3
CONNECT_MAXTIME	Zeitlimit für den Verbindungsstatus.	seconds	20…200	90
CONNECT_EXTENSION	Client-Zeitlimitverlängerung für den Verbindungsstatus.	seconds	1…60	30
WAIT_RECONNECT	Wartezeit für Wiederaufbau einer aufgebauten Verbindung (Verbindungssignal verloren).	seconds	3…30	10
DROPPED_RETRY	Wert, der die Zeit festlegt, in der der AP versucht, die vorherige Verbindung unter Verwendung der gespeicherten SSID und des Zugangsschlüssels erneut aufzubauen. Nach Ablauf dieser Zeit werden die alte SSID und der Zugangsschlüssel verworfen und der AP geht in den Zustand IDLE über.	times	1…10	5

6.1.8.5 Konfigurationshinweis Web-Interface

Wenn der ICCP-Prozess auf beiden Partnern aktiviert und konfiguriert ist, kann der Protokollstatus über die Weboberfläche auf der Hauptseite Status/advanced im Menüreiter ICCP beobachtet werden.



ICCP-Statusanzeige auf dem Webserver

6.1.8.6 VLAN über Funk ICCP

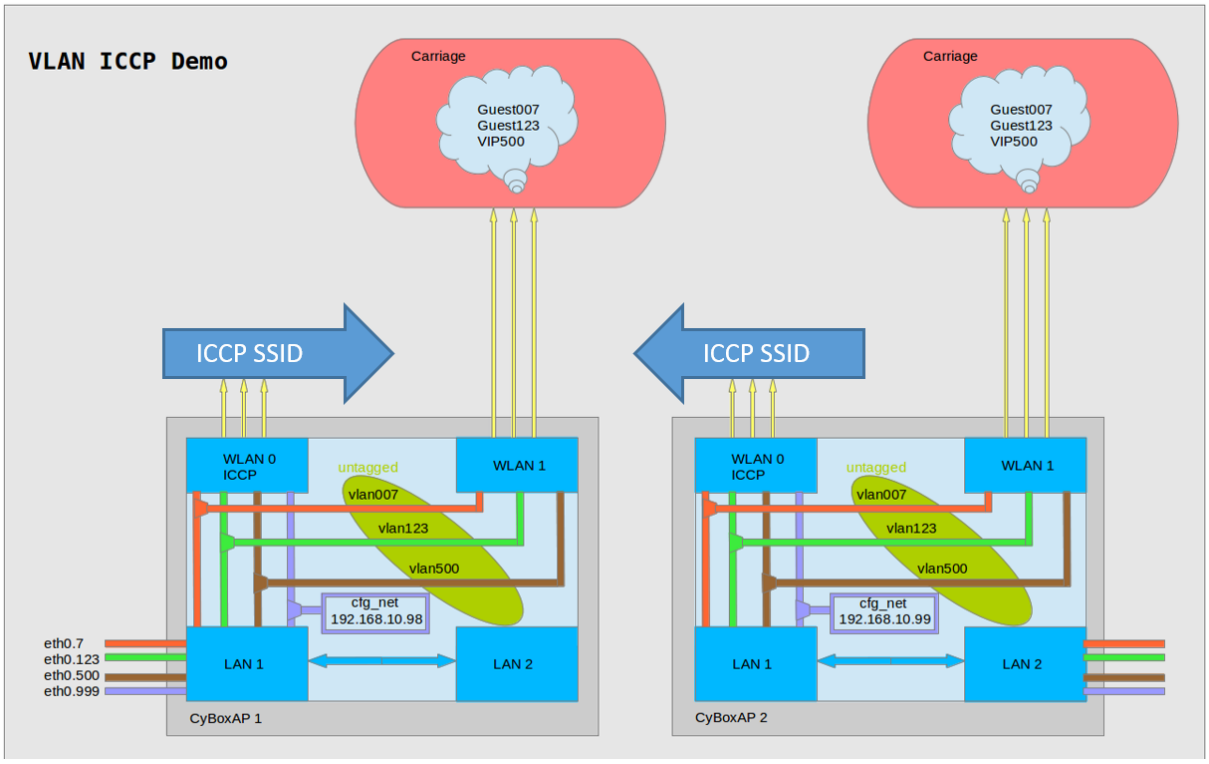
Die neueste ICCP-Implementierung wurde für den Einsatz in einer VLAN-Netzwerkumgebung erweitert. Dies kann die Netzwerksicherheit erhöhen, indem der Datenverkehr in verschiedene virtuelle Kanäle aufgeteilt wird, d.h. einen dedizierten Kanal für die Konfiguration und für Service Zwecke sowie beliebig weitere Kanäle bspw. für den Gastzugang und VIP-Zugang.

6.1.8.6.1 Funktionen und Einschränkungen

- Die native Schnittstelle ‚eth0' und die native Schnittstelle ‚wlan0/1' (die von ICCP verwendet wird) sind für weitere Bridge-Gerät nich mehr verfügbar.
- Die Backbone-VLAN-Netzwerke/Bridges müssen manuell konfiguriert werden. Jeder VLAN-Kanal benötigt eine eigene Netzwerkschnittstelle.
- Der Name der Netzwerkschnittstelle kann bis zu 7 Zeichen lang sein. Es können beliebige Zeichen verwendet werden, aber *Name* darf keine Teilfolge eines anderen Namens sein. z.B. ist eine Kombination aus ‚vlan1' und ‚vlan123' nicht zulässig. Die Namen sollten stattdessen ‚vlan001' und ‚vlan123' lauten.
- Die entsprechende Ethernet-Schnittstelle muss angelegt sein (z.B.; eth0.123 für vlan123).
- Alle VLAN-Kanäle (network name) auf dem Backbone müssen als kommaseparierte Liste im ICCP-Menüeintrag ‚Used vlan networks' exakt eingetragen werden.
- Das zweite WLAN-Modul, das nicht für ICCP verwendet wird, kann als Standard-Access-Point fungieren. Die SSIDs für dieses Modul müssen sich von jedem als ICCP-SSID verwendeten Namen unterscheiden. Der Verkehr auf diesen Access Point-SSIDs ist immer ungetaggt, wird aber getaggt, sobald die Pakete eine Backbone-Bridge erreichen. Jeglicher Verkehr auf dem Backbone ist getaggt.
- Sobald der Master-Kanal im etablierten Zustand ist, werden alle konfigurierten ‚Used VLAN networks' über Tunnel (d. h. gretap-Schnittstellen) gestartet. Nachdem alle Kanäle im etablierten Zustand sind, wird die Konfiguration dauerhaft gespeichert. So können sich die ICCP-Partner beim nächsten Hochfahren des Systems schnell wieder verbinden. Wenn die Verbindung abbricht und der Master-Kanal in den Idle-Zustand geht, werden die entsprechenden VLANs deaktiviert.

6.1.8.6.2 Beispiele

Abbildung 34 zeigt ein Beispiel für eine Konfiguration, die VLANs über ICCP verwendet.



ICCP-Darstellung für VLAN-Nutzung

Fall 1: Dynamische ICCP

Die Konfiguration muss auf beiden ICCP-Partnern durchgeführt werden.

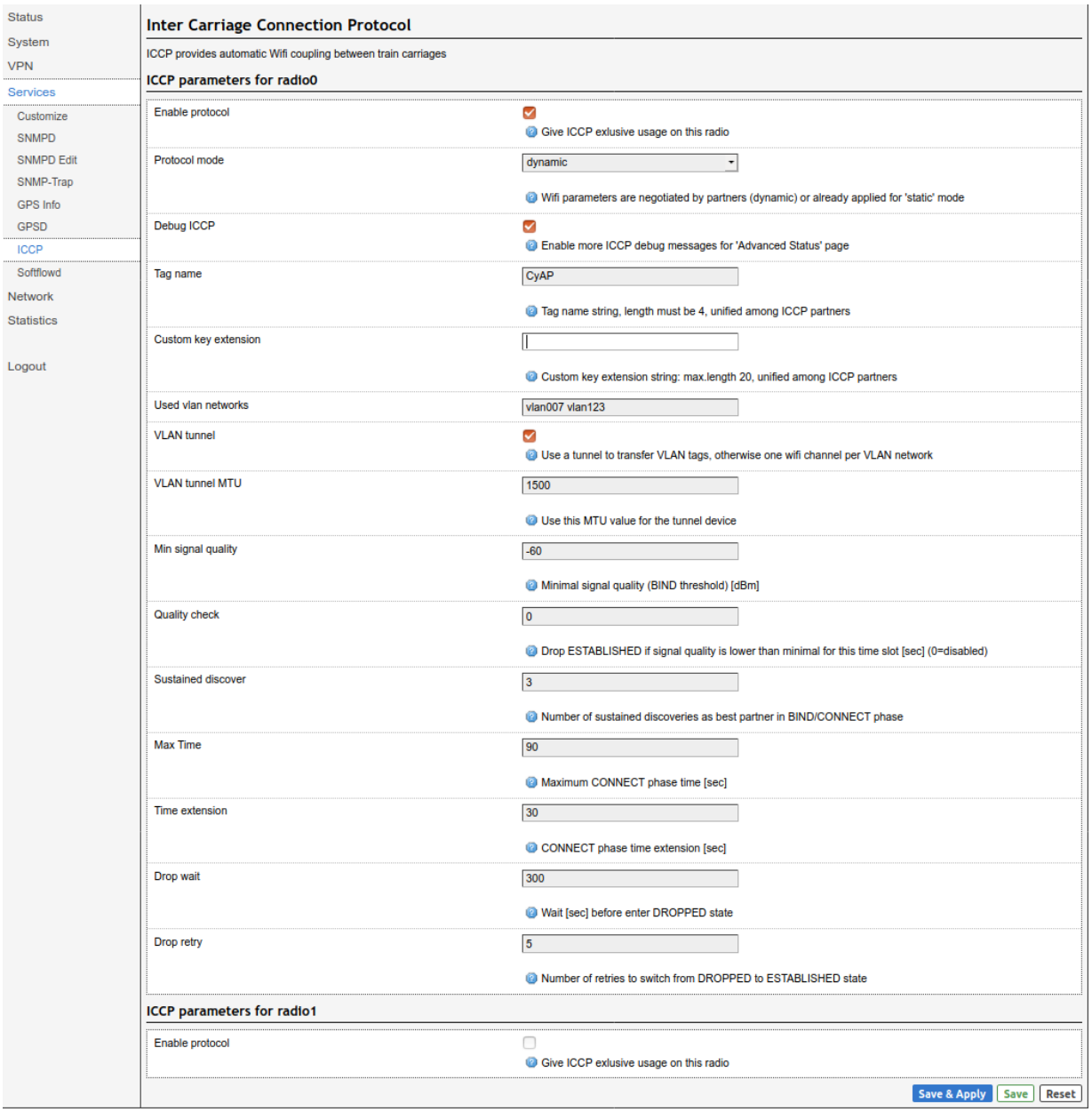
a. *Interface-Konfiguration*

Zusätzlich zu den Schritten, die in `Configurable Parameters` beschrieben sind, muss jedes VLAN (vlan007 und vlan123) wie folgt konfiguriert werden:

- Erstellen Sie eine neue Schnittstelle mit dem Namen - „vlan007“ auf der Registerkarte `Network` → Interfaces
- Wenn Sie aufgefordert werden, eine physikalische Schnittstelle anzugeben, erstellen Sie die benutzerdefinierte Schnittstelle mit dem Namen ‚*eth0.007*‘ und klicken Sie dann auf Save & Apply

b. *ICCP VLAN-Konfiguration*

ICCP kann über die Weboberfläche wie unten gezeigt oder über die Kommandozeile mit dem Befehl ‚cfg_iccp -d -p dynamic -r 0 -v vlan123 -v vlan007‘ konfiguriert werden.



Dynamische ICCP-VLAN-Konfiguration

Hinweis: Stellen Sie sicher, dass das Kontrollkästchen VLAN-Tunnel aktiviert ist.

Fall 2: Statische ICCP

Statisches ICCP kann verwendet werden, wenn keine Neukonfigurationen von Zugwaggons anstehen und die Endpunkte von VLAN-Tunneln zum Zeitpunkt der Konfiguration bereits bekannt sind.

Die Konfiguration muss auf beiden ICCP-Partnern durchgeführt werden.

a. *Interface-Konfiguration*

Zusätzlich zu den Schritten, die in `Configurable Parameters` beschrieben sind, muss jedes VLAN (vlan007 und vlan123) wie folgt konfiguriert werden:

- Erstellen Sie eine neue Schnittstelle mit dem Namen „vlan007“ auf der Registerkarte `Network` → `Interfaces`
- Wenn Sie aufgefordert werden, eine physikalische Schnittstelle anzugeben, erstellen Sie die benutzerdefinierte Schnittstelle eth0.007 und klicken Sie dann auf ‘*Save & Apply*’

Weitere Schritte sind auch bei der Konfiguration der ICCP-Management-Schnittstelle erforderlich:

- Die WLAN-Module beider ICCP-Partner müssen miteinander verbunden sein. Das bedeutet, dass auf einem Funkmodul der Modus „Access Point (WDS)“ und auf dem anderen Funkmodul der Modus „Client (WDS)“ gewählt werden muss. Alle anderen Parameter wie SSID, Verschlüsselung und Betriebsfrequenz müssen ebenfalls eingestellt werden, um die Verbindung wie bei einer Standard-Master/Client-WLAN-Verbindung zu gewährleisten. Alle diese Einstellungen können in der Registerkarte `Network` → `Wireless` konfiguriert werden.
- Für die ICCP-Management-Schnittstelle müssen in der Registerkarte ‘*Network*’ → ‘Interfaces’ statische IPs im gleichen Subnetz eingestellt werden (z.B. wenn das Lan-Interface als ICCP-Management-Interface inklusive eth0 und wlan0 ausgewählt ist, kann die IP-Adresse auf 10.0.0.1 bei „ICCP-Partner A“ und auf 10.0.0.2 bei „ICCP-Partner B“ eingestellt werden).

b. *ICCP VLAN-Konfiguration*

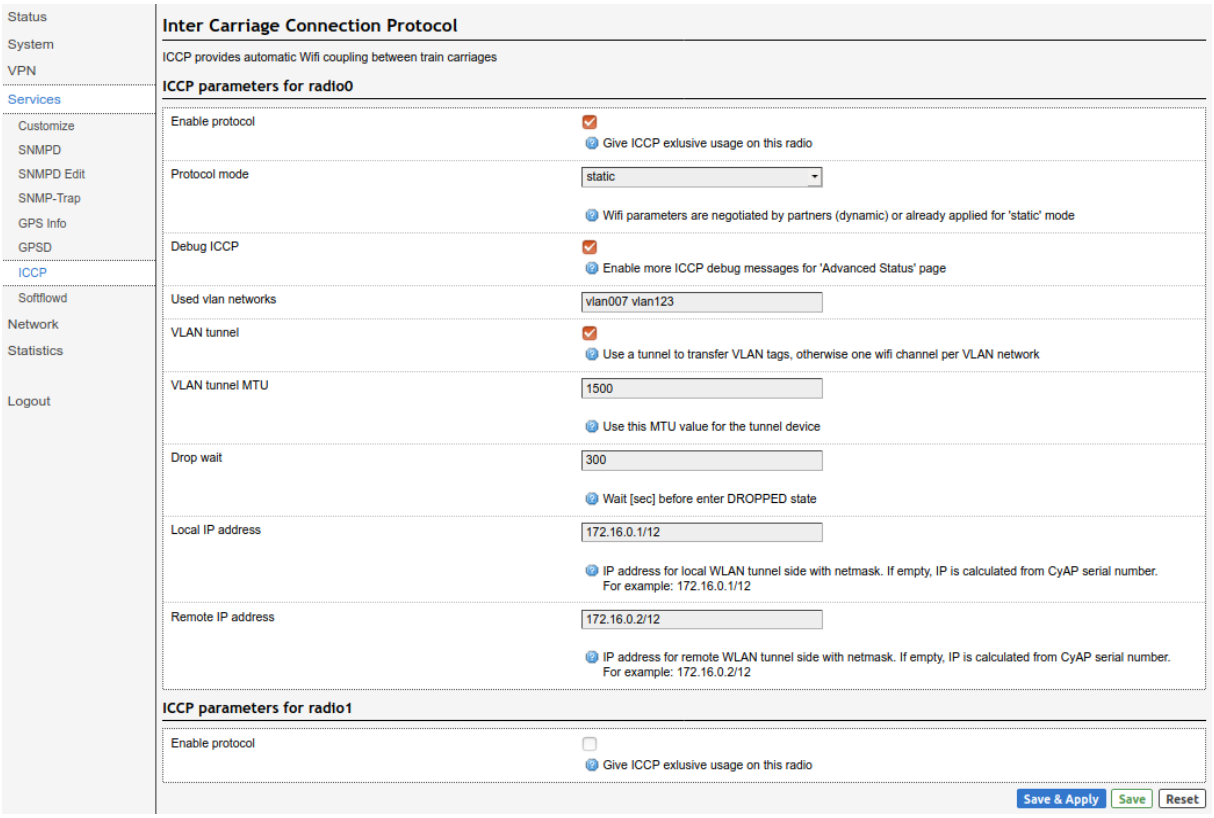
ICCP kann über die Weboberfläche wie unten gezeigt oder über die Kommandozeile mit den folgenden Befehlen konfiguriert werden:

Auf 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

Auf 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



Statische ICCP-VLAN-Konfiguration

Hinweis 1: Das Kontrollkästchen VLAN-Tunnel sollte aktiviert sein.

Hinweis 2: Die Felder für die lokale und die entfernte IP-Adresse müssen bei der Verbindung ICCP-Partner ausgetauscht werden. Die lokale IP ist diejenige, die auf der ICCP-Verwaltungsschnittstelle auf dem Access Point eingestellt ist, den Sie gerade konfigurieren. Der obige Screenshot gilt für ICCP-Partner A.

6.1.9 QoS

Im folgenden Beispiel wird eine Netzwerkschnittstelle LAN oder WLAN für die Verwendung der Quality-of-Service-Funktion (QoS) vorbereitet. Die CyBox AP 2 implementiert eine QoS-Funktion mit Skripten zur Konfiguration der Verkehrssteuerung (‚tc'-Befehl), die den Durchsatz an einer ausgewählten Schnittstelle reduziert. Um den Effekt zu sehen, kann ein Leistungstest mit dem eingebauten Programm ‚iperf' gestartet werden, um den Durchsatz zu messen.

- Wählen Sie `Network` → `QoS`
- Die Standard-‚Schnittstelle' WAN ist nicht aktiviert und kann gelöscht werden.
    - Geben Sie im Feld Interfaces einen bestehenden Schnittstellennamen ein, z. B. ‚lan', und klicken Sie auf die Schaltfläche Hinzufügen Add
        - Geben Sie im Feld Download speed (kbit/s) 1024 ein
        - Geben Sie im Feld Upload speed (kbit/s) 1024 ein
        - AcAktivieren Sie die Checkbox Enable
    - Klicken Sie `Save & Apply`

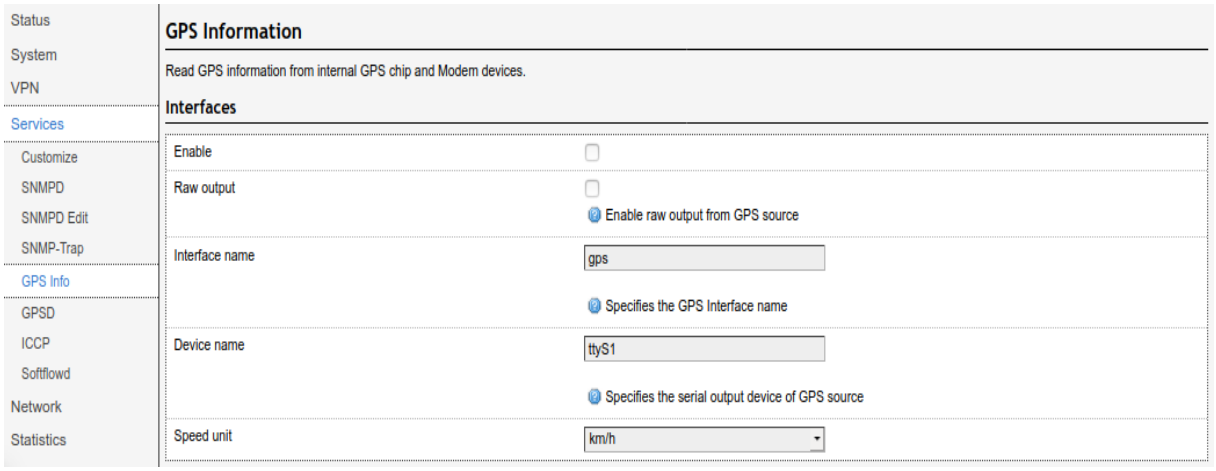
Führen Sie einen ‚iperf'-Leistungstest durch. Der Durchsatz sollte etwa 10 Mbits/s betragen. Wenn eine WLAN-Schnittstelle mit dem LAN-Port gebrückt ist, kann die Verkehrssteuerung sogar auf einem einzelnen Teil der Brücke funktionieren. Um nur den WLAN-Verkehr zu reduzieren, muss im Menü `Network` → `Interfaces` ein neues Schnittstellen-Label hinzugefügt werden, z.B. WLAN. Dann muss das neue Schnittstellen-Label im QoS-Menü verwendet werden.

6.2 GPS

Einige Mitglieder der CyBox-Familie sind mit einem zusätzlichen GNSS-Hardwaremodul ausgestattet. Die GPS-Antenne wird auf die Frontplatte geführt. Sobald eine entsprechende Antenne angeschlossen ist, wird das GPS-Signal empfangen und kann verarbeitet werden, wenn eine Version V3.03 oder neuer installiert ist. Die GPS-Hardware liefert auf der zweiten seriellen Schnittstelle das NMEA 0183-Protokoll, das in eine menschenlesbare Form umgewandelt wird.

6.2.1 GPS-Aktivierung

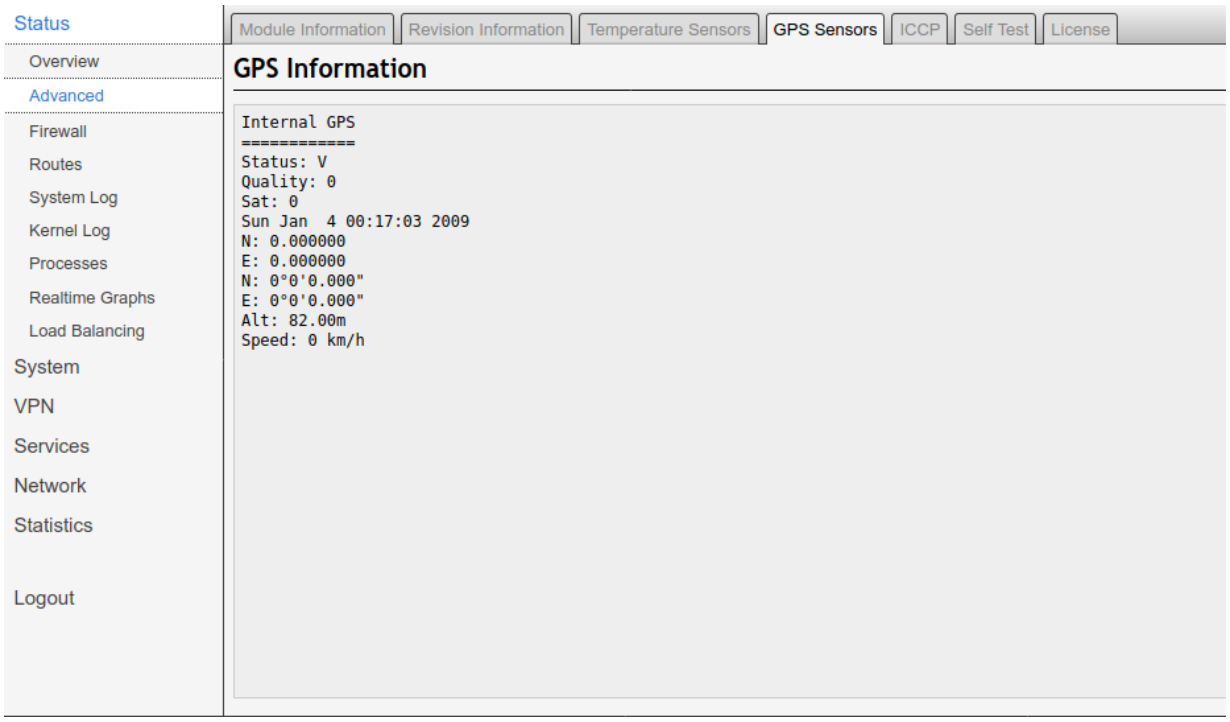
Das GPS ist standardmäßig deaktiviert. Es kann über die Weboberfläche aktiviert werden. Geben Sie auf `System` → `GPS Info` und markieren Sie Enable.



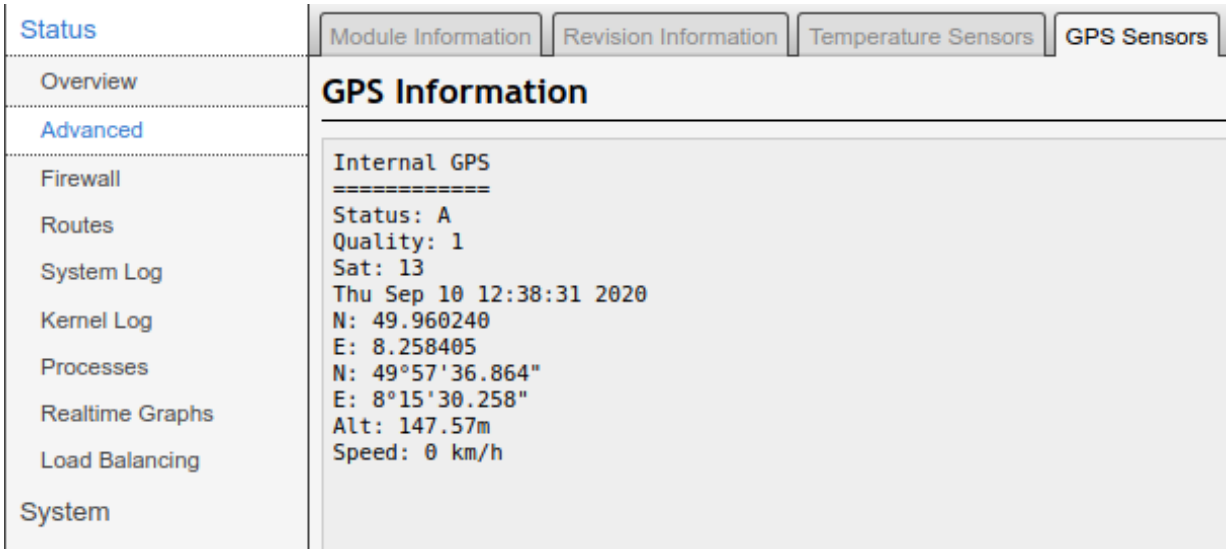
GPS-Aktivierung

6.2.2 GPS-Status

Die GPS-Informationen werden auf dem `Status` → `Advanced` der Weboberfläche angezeigt. Die nächste Abbildung zeigt ein Beispiel, das unmittelbar nach dem Hochfahren verfügbar ist. Und die untere Abbildung zeigt den gleichen Status, nachdem der Empfänger sich selbst kalibriert hat. Die Tabelle unten bietet eine Interpretation der GPS-Statusdaten.



GPS-Info sofort nach dem Start



Zuverlässige GPS-Informationen nach Hardware-Kalibrierung

GPS-Statusdaten:

Data Item	Wert	Beschreibung
Integrity	A	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

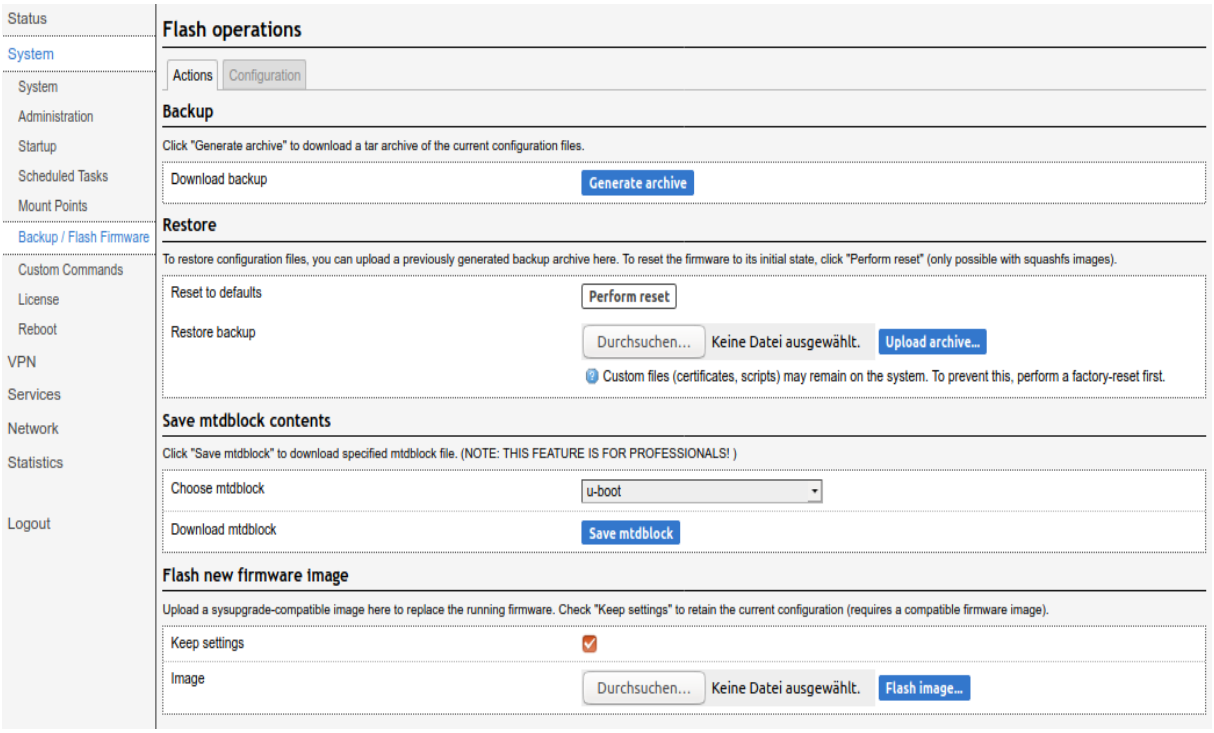
6.2.3 SNMP für GPS

Siehe Kapitel SNMP-Unterstützung für GPS

6.3 System

6.3.1 Sicherungen der Konfiguration

Die Konfiguration wird in der Registerkarte `System` → `Backup/Flash Firmware` verwaltet.



Konfiguration der Sicherungseinstellungen

a. Werkseinstellungen wiederherstellen

Reset durchführen stellt die Werkseinstellungen wieder her und führt einen Neustart durch.

b. Konfiguration exportieren

Verwenden Sie die Schaltfläche Generate archive, um eine Konfigurationssicherung zu exportieren.

Das generierte Konfigurations-Tar-Archiv ist nicht hardwarespezifisch und kann an andere Access Points weitergegeben werden, solange diese das gleiche Modell und die gleiche Firmware-Version haben.

Hinweis: Konfigurationsarchive sind nicht kompatibel zwischen den Firmware-Revisionen 4.x und 17.xx.yy.

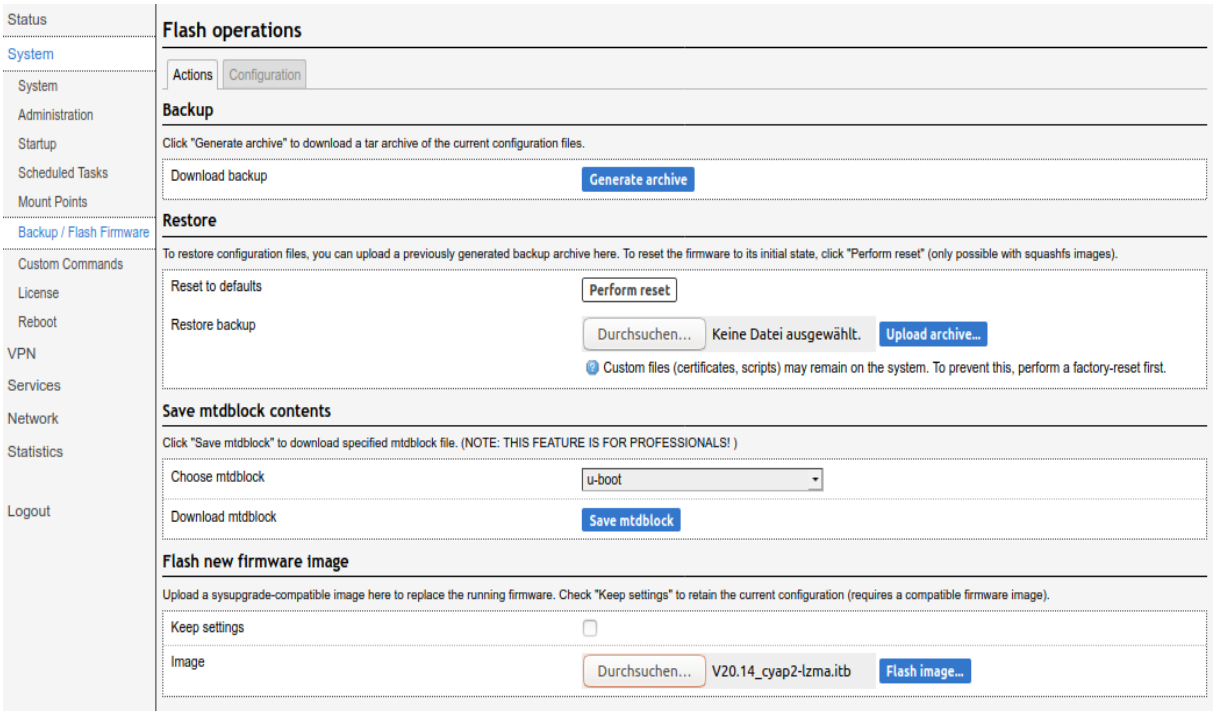
Mit der Schaltfläche Upload archive… können Sie eine zuvor gespeicherte Konfiguration wiederherstellen. Nach dem Wiederherstellen einer Konfiguration wird der Access Point neu gestartet.

c. Konfiguration importieren

Bevor Sie ein Konfigurationsarchiv wiederherstellen, stellen Sie sicher, dass die Werkseinstellungen wiederhergestellt wurden, um Konflikte zwischen Ihrer alten und neuen Konfiguration zu vermeiden. Die Konfigurationsdatei muss nach dem Muster backup-*.tar.gz benannt sein und kann dann im Feld Restore backup hochgeladen werden.

6.3.2 Firmware-Upgrade

Die Vorgehensweise zum Aktualisieren der Gerätefirmware mit einem neuen Image wird im Folgenden gezeigt.



Firmware-Update-Einstellungen

Firmware-Updates werden als Binär-Images mit der Endung .itb zur Verfügung gestellt und werden vom Host-Computer hochgeladen. Die Einstellungen sollten immer **cleared** werden, um sicherzustellen, dass alte und neue Konfigurationsschalter nicht verwechselt werden. Das hochgeladene Image hat eine MD5-Prüfsumme, die im folgenden Dialog bestätigt werden muss.

WARNUNG: Schalten Sie den Access Point NICHT AUS, während Sie die Firmware aktualisieren bzw. wiederherstellen und flashen. Denken Sie daran, dass, wenn das Kontrollkästchen ``Keep settings`` deaktiviert ist, das Gerät nach dem Neustart zu seiner Netzwerk-Standardadresse zurückkehrt.

6.3.3 Neustart

Das Gerät kann auf der Registerkarte `System` → `Reboot` neu gebootet werden.

6.3.4 Reset-Taste

Die Vorgänge, die mit der Reset-Taste durchgeführt werden können, sind: Neustart (reboot), Auslösen des Notfallmodus (triggering the emergency mode, Wiederherstellen der Werkseinstellungen (restoring factory settings).

a. Werkseinstellungen wiederherstellen

Nach dem Booten kann ein Werksreset ausgelöst werden, indem der Reset-Taster mit einem Stift länger als 5 Sekunden gedrückt wird. Die Fail-LED blinkt grün und nach ein paar Sekunden startet das Gerät mit der Standardkonfiguration neu.

Ein Neustart kann durch Drücken der Reset-Taste mit einem Stift für weniger als 2 Sekunden ausgelöst werden.

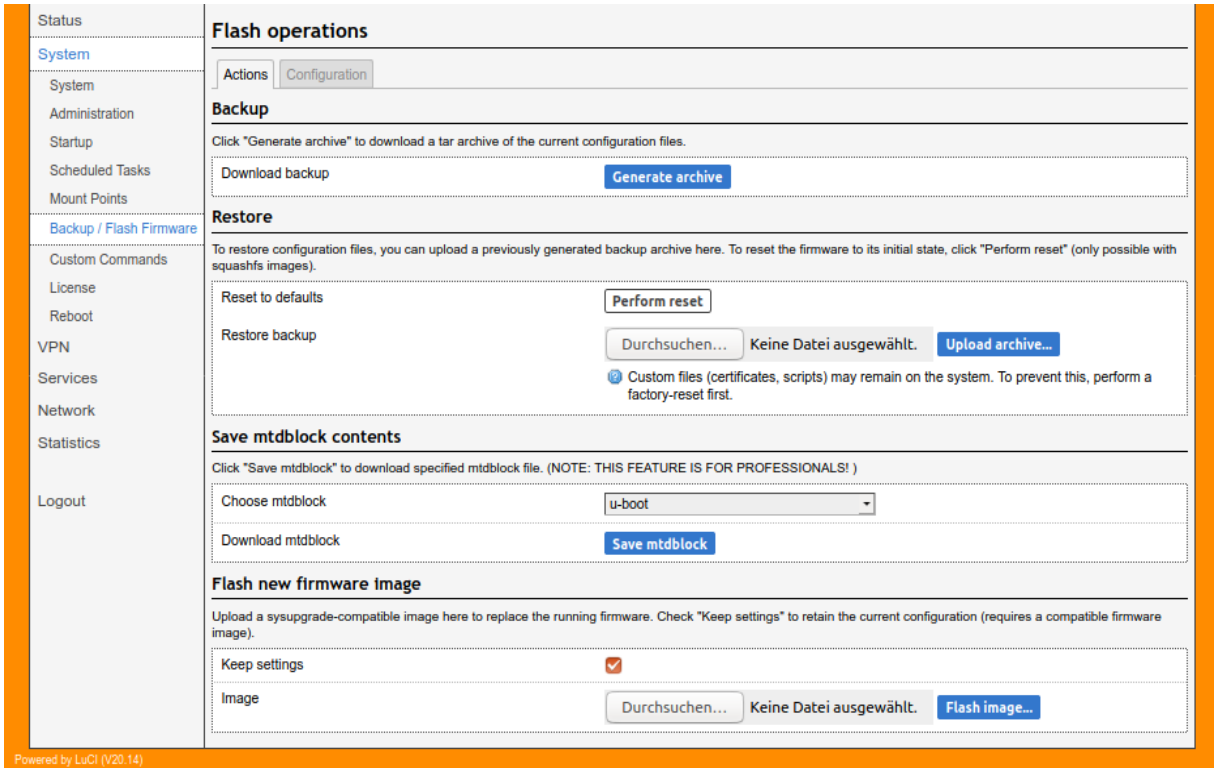
6.3.5 Notfall-Modus

Der Notfallmodus sollte nur im Falle eines System-Firmware-Upgrades oder einer Crash-Wiederherstellung benötigt werden.

Die CyBox AP-Familie verwendet mindestens fünf Partitionen im Flash-Speicher. Das erste Flash-Gerät enthält das Low-Level-Firmware U-Boot, das zweite Flash-Gerät ein Notfall-Image von OpenWrt/Linux und das dritte

Gerät das Standard-Image von OpenWrt/Linux. Das vierte Flash-Gerät enthält eine Journaling-Flash-Dateisystempartition mit Benutzerkonfigurationseinstellungen sowie eine Kundenpartition. Normalerweise wird das Standard-OpenWrt/Linux-Image mit U-Boot geladen und mit MD5-Summen auf Fehler geprüft. Wenn die Prüfsummen gültig sind, bootet das Linux und der Access Point-Service startet. Die Benutzerkonfigurationsparameter werden von der JFFS-Partition geladen und angewendet.

Im Falle eines beschädigten Standard-Images (OpenWrt/Linux im dritten Flash) erkennt U-Boot einen MD5-Prüfsummenfehler und versucht, das Not-System-Image aus dem zweiten Flash zu starten. Während des Bootens werden keine Benutzerkonfigurationseinstellungen übernommen. Die CyBox AP 2 meldet sich mit der Netzwerk-Standardadresse 192.168.100.1 (user=root, password=root) und deaktiviertem Wifi. Die Fail-LED blinkt orange (rote und grüne LED leuchten) und der Hintergrund der Weboberfläche ist orange, wie in der Abbildung dargestellt. Alle Konfigurationseinstellungen sind volatil. Dieses System sollte nur zum Upgrade/Wiederherstellen eines funktionierenden Firmware-Images auf ein zweites Flash über das Menü *Backup / Flash Firmware* verwendet werden.



Anzeige des Notfallsystems

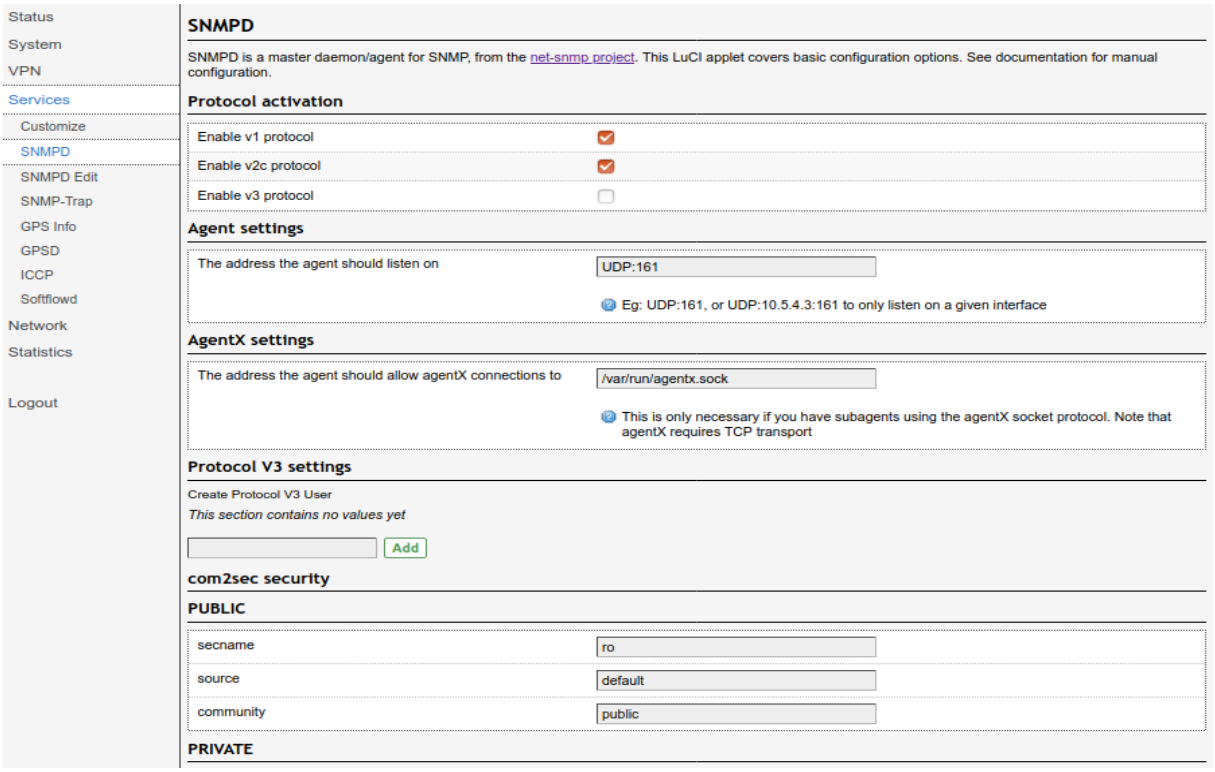
Der Notfallmodus kann auch aufgerufen werden, indem Sie zu Beginn der Boot-Phase die Reset-Taste 5 Sekunden lang gedrückt halten.

Hinweis: Normalerweise zeigt der blaue Hintergrund den Standardmodus und der orange Hintergrund den Notfallmodus an. Viele Webbrowser halten die Farben jedoch im Cache, wodurch die falsche Farbe angezeigt werden kann. Um sicherzustellen, dass die richtige Farbe angezeigt wird, öffnen Sie ein neues Fenster im privaten oder Inkognito-Modus, bevor Sie die Weboberfläche aufrufen.

7 SNMP

7.1 SNMP-Protokoll-Unterstützung

Firmware-Implementierungen vor 2020 haben nur Protokollunterstützung für Version **v1** und **v2c**. Seit 2020 ist auch das SNMP-Protokoll **v3** in jeder CyBox-Firmware enthalten. Die Protokollvarianten **v1**, **v2c** sind in der Werkseinstellung vorhanden. In der Werkseinstellung ist nur der `read` Zugriff erlaubt



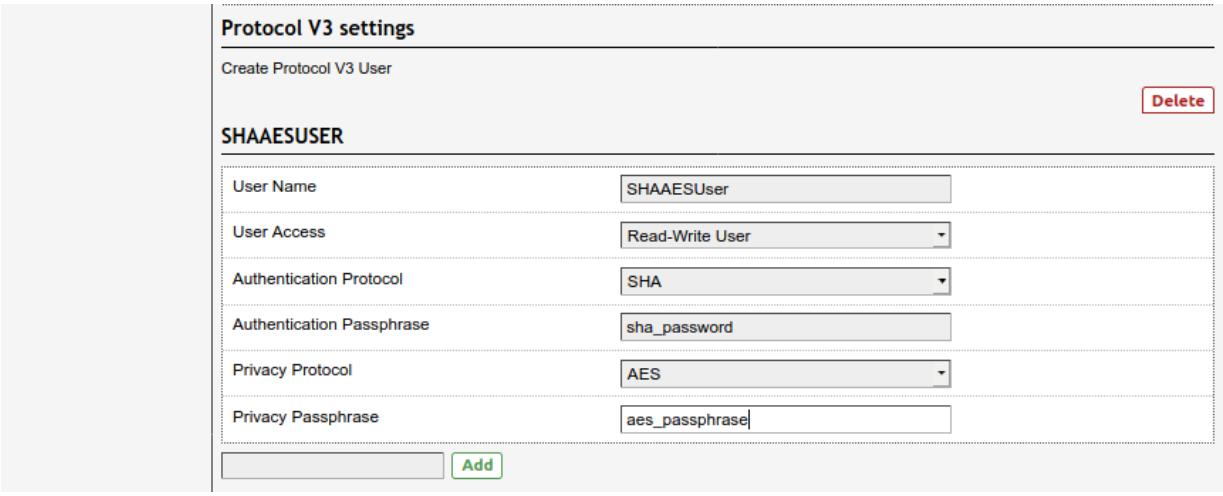
SNMPD-Werkseinstellungen mit aktiviertem Protokoll v1 und v2c

7.2 Unterstützung des SNMP V3-Protokolls

Bevor ein **v3**-Protokollzugriff ausgeführt werden kann, müssen ein oder mehrere V3-Benutzerkonten angelegt werden. Um ein neues **v3**-Benutzerkonto hinzuzufügen, muss der Name `case sensitiv` eingegeben werden. Später zeigt die WUI den Namen des Benutzerkontos in Großbuchstaben an.

Neues v3-Benutzerkonto anlegen

Das neue Benutzerkonto kann als `read-only` oder mit `read-write`-Berechtigung angelegt werden. Das Authentifizierungsprotokoll ist entweder **MD5** oder **SHA** (preferred). Wenn ein Authentifizierungsprotokoll ausgewählt wird, muss auch die Authentifizierungspassphrase angegeben werden. Für die Verschlüsselung des Datenpakets wählen Sie **DES** oder **AES** (preferred) und geben ebenfalls eine Passphrase an. Verwenden Sie zur Veranschaulichung die gleichen Einstellungen wie in der Abbildung unten, um sie in die Beispiele zu kopieren und einzufügen.



Einstellungen des Demo-Benutzerkontos

Die Standardprotokolle **v1** und **v2c** sollten bei Verwendung des SNMP-V3-Protokolls deaktiviert werden.

Nur SNMP-V3-Protokoll aktivieren

Nachdem alle neuen Einstellungen eingegeben wurden, drücken Sie die Taste `Save & Apply`. Danach wird der SNMPD-Dienst automatisch neu gestartet.

7.2.1 SNMP V3-Protokoll-Beispiele

Lesezugriff mit **snmpget**: `Get order identifier` (Auftragskennung holen)

Der Befehl:

```
snmpget  -v 3 -n "" -u SHAAESUser -a SHA -A "sha_password" -x AES -X "aes_passphrase" -l authPriv
192.168.100.1     1.3.6.1.4.1.2021.8.1.2.100.101.1
```

Rückgabe:

```
iso.3.6.1.4.1.2021.8.1.2.100.101.1 = STRING: "CYAPW-1057P0"
```

Lesezugriff mit **snmpwalk**: `Get firmware version` (Firmware-Version abfragen)

Der Befehl:

```
snmpwalk  -v 3 -n "" -u SHAAESUser -a SHA -A "sha_password" -x AES -X "aes_passphrase" -l authPriv
192.168.100.1     1.3.6.1.4.1.2021.8.1.2.103
```

Rückgabe:

```
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"
```

```
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 = ""
```

Schreibzugriff mit **snmpset**: `Set a new system hostname and reload system settings` (Setzen eines neuen System-Hostnamens und Neuladen der Systemeinstellungen)

Verwenden Sie die folgende Reihenfolge, um den neuen Hostnamen einzustellen:

```
snmpset  -v 3 -n "" -u SHAAESUser -a SHA -A "sha_password" -x AES -X "aes_passphrase" -l authPriv
192.168.100.1    1.3.6.1.4.1.2021.8.1  s "uci set system.@system[0].hostname=Brutus"

iso.3.6.1.4.1.2021.8.1 = STRING: "uci set system.@system[0].hostname=Brutus"

snmpset  -v 3 -n "" -u SHAAESUser -a SHA -A "sha_password"  -x AES -X "aes_passphrase" -l authPriv
192.168.100.1    1.3.6.1.4.1.2021.8.1  s "uci commit system"

iso.3.6.1.4.1.2021.8.1 = STRING: "uci commit system"

snmpset  -v 3 -n "" -u SHAAESUser -a SHA -A "sha_password"-x AES -X "aes_passphrase" -l authPriv
192.168.100.1    1.3.6.1.4.1.2021.8.1  s "service system reload"

iso.3.6.1.4.1.2021.8.1 = STRING: "service system reload"
```

Der neue System-Hostname kann auf der Web-Statusseite überprüft werden.

7.3 SNMP-Grundfunktionen

Der SNMP-Dienst ist in der CyBox AP 2 ab der Firmware-Version 2.6 enthalten. Der Dienst ist aktiviert, wenn eine gültige Konfigurationsdatei ‚/etc/config/snmpd' vorhanden ist und der Dienststart nicht deaktiviert ist. Beim Systemstart wird diese Konfigurationsdatei geparst und in eine ‚snmpd.conf'-Datei übersetzt, die vom SNMP-Daemon benötigt wird. Die ‚snmpd.conf' wird in ‚/var/run' gespeichert und ein symbolischer Link ist unter ‚/etc/snmp' vorhanden.

Es gibt eine grundlegende Webschnittstelle für die SNMP-private/public-Konfiguration unter Services → SNMPD. Die gesamte Konfigurationsdatei ist recht groß (~120KB) und kann auf der Kommandozeile mit UCI-Befehlen oder durch Editieren der Konfigurationsdatei in Editierfenster Services → SNMPD-Edit geändert werden. Die aktuelle Implementierung wird automatisch von einem Build-Skript generiert.

Die OpenWrt-Standardkonfiguration bietet einen Satz von Standard-MIB-Dateien mit der OID .1.3.6.1.2.1 (iso.org.dod.internet.mgmt.mib-2). ELTEC stellt auch eine Erweiterung für die Standardkonfiguration zur Verfügung, die das UC DAVIS (University of California, Davis) MIB-Objekt (UCD-SNMP-MIB MIB-Dokument als .1.3.6.1.4.1.2021) verwendet, um viele Konfigurationseinstellungen mit einer Wrapper-Shell zum Lesen ‚/usr/sbin/get_snmp' und zum Schreiben ‚/usr/sbin/get_snmp' einzelner Einträge in den Konfigurationsdateien unter ‚/etc/config' abzubilden. Das Skript ‚get_snmp' liefert auch Informationen über die Zuordnung von WLAN zu SSID, WLAN-Bitraten, Signalqualität, etc. Die meisten dieser Informationen werden über UCI-Befehle zum Lesen und Schreiben von Systemkonfigurationseinstellungen gewonnen.

/etc/snmp/snmpd.conf # Symlink zur SNMPD-Konfigurationsdatei (wird automatisch erstellt)

/etc/config/snmpd # OpenWrt-Konfigurationsdatei

In Anhang 10 finden Sie eine Übersicht der SNMP-Befehls-OIDs.

7.4 SNMP Lese- und Schreibberechtigungen

Auf der CyBox AP 2 läuft ein lokaler SNMP-Daemon, der derzeit für zwei Zugriffsgruppen konfiguriert ist:

- Standardmäßig erlaubt die Gruppe „public" uneingeschränkten Read-only-Zugriff

- Die Gruppe „private“ erlaubt einem einzelnen angegebenen Host das Lesen und Schreiben. Standardmäßig ist „localhost“ angegeben, d.h. nur der lokale administrative Benutzer auf der CyBox AP 2 ist für SNMP-Schreiboperationen zugelassen.

Diese Adresse kann mit Hilfe eines UCI-Befehls geändert werden. Angenommen, Sie sind auf einer CyBox AP 2 über SSH als administrativer Benutzer angemeldet, dann würde der folgende Befehl die Neufestlegung der IP-Adresse der „private“-Gruppe ermöglichen:

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

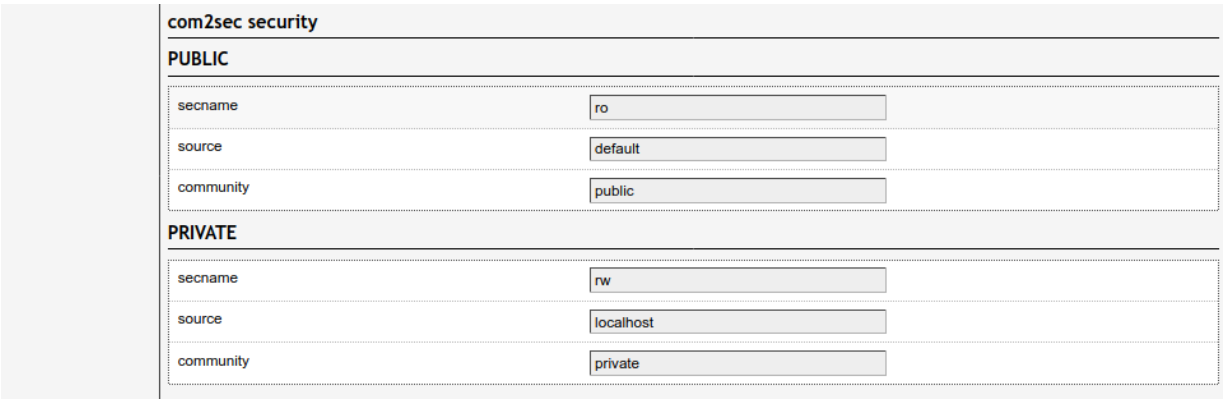
Dabei bezieht sich *<ccu>* auf die IP-Adresse (oder den Hostnamen) des entfernten Hosts, der SNMP-Schreiboperationen durchführen darf. Das Schlüsselwort „default“ anstelle einer bestimmten Adresse erlaubt beliebigen Hosts den Zugriff auf den SNMP-Dämon.

Ebenso kann die Adresse der „public“-Gruppe geändert werden:

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

Hinweis: Im Allgemeinen sollten lokale UCI-Befehle auf der CyBox AP 2 für die Handhabung der Konfiguration des SNMP-Dämons verwendet werden. Führen Sie *‚uci show snmpd‘* aus, um die aktuellen Einstellungen anzuzeigen.

Alternativ können die öffentlichen und privaten Quellen mit der Weboberfläche im Feld *‚com2sec security‘* des Reiters *‚Services‘* → *‚SNMPD‘* geändert werden.



SNMPD-Änderung ‚com2sec security‘ für Schreibzugriff

7.5 SNMP-Befehle

Der SNMP-Dämon der CyBox AP 2 unterstützt die folgenden Befehle:

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

Ein Sonderfall tritt auf, wenn snmpset auf Nicht-MIB-Erweiterungen schreibt. In diesem Fall besteht eine Asymmetrie zwischen snmpget und snmpset in Bezug auf OIDs. Das Lesen (snmpget) erfordert den vollständigen numerischen Identifier einschließlich der serverspezifischen Erweiterung. Schreiben (snmpset) akzeptiert nur den „extEntry“-Stamm „iso.3.6.1.4.1.2021.8.1“, während der serverspezifische Name des Objekts als erstes Argument übergeben werden muss.

Die Zuordnung von Namen und OID-Nummern kann durch Ausführen von snmpwalk ermittelt werden.

7.6 SNMP-Lesen (snmpwalk und snmpget)

In den folgenden Kapiteln wird der Lese- und Schreibzugriff über Konsolenbefehle beschrieben.

7.6.1 Lesen von Systeminformationen

```
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
custom1 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
```

Der Befehl

```
snmpwalk -c public -v 2c 192.168.100.1 1.3.6.1.4.1.2021.8.1.2.100
```

liefert

```
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"
```

Funktion ausgeführt auf der CyBox AP 2:

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

Fehlercode aus Funktionsaufruf:

```
iso.3.6.1.4.1.2021.8.1.2.100.100.1 = INTEGER: 0
```

Rückgabewert vom Funktionsaufruf:

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

7.6.2 Lesen von SNMP-Objektinformationen

Das Hauptproblem beim Zugriff auf ein Netzwerkgerät (WLAN oder LAN) ist, dass die Reihenfolge der Auflistung von der Erstellungsreihenfolge abhängt, die der Benutzer beim Bearbeiten der Konfigurationsdatei festgelegt hat. Die Tatsache, dass die Network-/Interface-Namen frei wählbar sind und die UCD-MIB-Objektnamen statisch sind, macht es notwendig, vordefinierte Namen zu verwenden, wie z.B.:

- network0, network1 … network9
- wireless0, wireless1 … wireless19

Hinweis: Eine normale CyBox AP 2-Konfiguration besteht aus sechs Funk- Schnittstellen, aber es sind bis zu zwanzig Schnittstellen möglich, sodass snmpwalk bis zu 80 Prozent undefinierte Werte (leerer UCI-Eintrag) ergibt.

Die folgenden Objekte sind verfügbar, um die aktuelle Netzwerk-/Funkbefehle zu ermitteln.

7.6.2.1 Ausgabe des aktuellen Netzwerkgerätbefehls

Der Befehl

```
snmpwalk -c public -v 2c 192.168.100.1 1.3.6.1.4.1.2021.8.1.2.150
```

liefert

```
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: "vlan123=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.3.6.1.4.1.2021.8.1.2.150.102.1 = INTEGER: 0
iso.3.6.1.4.1.2021.8.1.2.150.103.1 = ""
```

Beispiel:

Die IP-Adresse der LAN-Schnittstelle ‚cfg_net' wird sein (network5 beginnt bei 550):

```
network5.ipaddr 1.3.6.1.4.1.2021.8.1.2.552
```

Der Befehl

```
snmpget -c public -v 2c 192.168.100.1 1.3.6.1.4.1.2021.8.1.2.552.101.1
```

liefert

```
iso.3.6.1.4.1.2021.8.1.2.552.101.1 = STRING: "192.168.99.98"
```

7.6.2.2 Ausgabe des SSID/WIFI-Interface-Befehls

Der folgende Befehl zeigt die Reihenfolge der Wifi-Schnittstellen.

```
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_vlan123**" <--- wireless3**
iso.3.6.1.4.1.2021.8.1.2.151.101.5 = STRING: "CyAP0_00486889_00486886_vlan500" **<--- wireless4**
iso.3.6.1.4.1.2021.8.1.2.151.101.6 = STRING: "CyAP0_00486889_00486886_cfg_net" **<--- wireless5**
iso.3.6.1.4.1.2021.8.1.2.151.101.7 = STRING: "Guest_123" **<--- wireless6**
iso.3.6.1.4.1.2021.8.1.2.151.101.8 = STRING: "VIP_500" **<--- wireless7**
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 Ausgabe Netzwerkgerät an SSID-Zuordnung

Der folgende Befehl zeigt die Reihenfolge der Wifi-Schnittstellen.

```
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: "wlan0-1 : \\"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: "wlan1 : \\"Guest_007\\""
iso.3.6.1.4.1.2021.8.1.2.152.101.7 = STRING: "wlan1-1 : \\"Guest_123\\""
iso.3.6.1.4.1.2021.8.1.2.152.101.8 = STRING: "wlan1-2 : \\"VIP_500\\""
iso.3.6.1.4.1.2021.8.1.2.152.102.1 = INTEGER: 0
iso.3.6.1.4.1.2021.8.1.2.152.103.1 = ""
```

Hinweis 1: Diese Zuordnung kann sich jedes Mal ändern, wenn eine bestimmte SSID deaktiviert oder aktiviert wird und die Funkschnittstelle neu gestartet wird. Das entsprechende Linux-WLAN-Gerät für eine SSID wird benötigt, um aktuelle Assoclist-, Bitraten- und Signalqualitätswerte auszulesen.

Hinweis 2: Die Auftrags-/Zuordnungsfunktionen (order/assignment) 150, 151 und 152 sollten in einer Applikation nicht gepollt werden, da sie einige CPU-Ressourcen benötigen. Der Netzwerkstatus sollte nur einmal nach dem Systemstart und immer dann ausgelesen werden, wenn ein Bediener eine Änderung des Netzwerk-Layouts veranlasst.

Beispiel:

Ausgabe von Assoclist, Bitrate und Signalqualität von 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
```

Der Befehl

```
snmpget -c public -v 2c 192.168.100.1 1.3.6.1.4.1.2021.8.1.2.202.101.1
```

gibt die Assoclist zurück

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

Der Befehl

```
snmpget -c public -v 2c 192.168.100.1 1.3.6.1.4.1.2021.8.1.2.242.101.1
```

gibt die Bitrateninformationen zurück

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

Der Befehl

```
snmpget -c public -v 2c 192.168.100.1 1.3.6.1.4.1.2021.8.1.2.282.101.1
```

liefert die Informationen zur Signalqualität

```
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-Schreiben (snmpset)

Standardmäßig ist die gesamte SNMP-Schreibsteuerung auf localhost beschränkt. Lesen Sie in Kapitel 8.1 nach, um den Schreibzugriff zu aktivieren.

Ein Schreibbefehl auf der CyBox AP 2 erfolgt immer auf die gleiche UCD MIB OID ‚1.3.6.1.4.1.2021.8.1'. Der Schreibvorgang erfordert einen String-Parameter, der mit ‚/etc/snmp/set_cyboxap' geparst und in einen systeminternen Aufruf auf der CyBox AP 2 übersetzt wird. Beachten Sie, dass alle Schreibvorgänge auf ein Konfigurationselement dauerhaft im Overlay-Dateisystem gespeichert werden und nach dem nächsten Stromzyklus vorhanden sind.

Verwendung des Systemaufrufs SNMPSET:

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

Der angegebene Parameterstring kann z. B. sein:

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

7.7.1 Direkter Befehl

7.7.1.1 Neustart

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

7.7.2 Konfiguration über Object Identifier (OID) bearbeiten

7.7.2.1 Einstellen einer neuen IP-Adresse

```
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 Einstellen einer neuen 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.3.6.1.4.1.2021.8.1.2.151.101.3 = STRING: "CyAP0_00486889_00486886_vlan007"
iso.3.6.1.4.1.2021.8.1.2.151.101.4 = STRING: "CyAP0_00486889_00486886_vlan123"
iso.3.6.1.4.1.2021.8.1.2.151.101.5 = STRING: "CyAP0_00486889_00486886_vlan500"
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.3.6.1.4.1.2021.8.1.2.151.101.8 = STRING: "VIP_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 = ""
```

Funkmodul aus wireless6.device=1.3.6.1.4.1.2021.8.1.2.1440 holen (kann weggelassen werden, wenn SSID-Radio bekannt ist):

```
snmpget -c public -v 2c 192.168.100.1 1.3.6.1.4.1.2021.8.1.2.1440.101.1
```

liefert

```
iso.3.6.1.4.1.2021.8.1.2.1440.101.1 = STRING: "radio1"
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 Einstellen eines neuen Macfilters

Wenden Sie einen neuen ‚macfilter' auf den Access Point „VIP_500" an. Bestimmte Benutzermakros sind ausgeschlossen.

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

Einzelbenutzer:

```
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"
```

Mehrere Benutzer:

```
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 Konfigurationsparameter bearbeiten, neue Felder anlegen und Elemente löschen

Wenn eine ‚config.section.option' bekannt ist, kann mit dem Befehl ‚uci set' ein beliebiges vorhandenes Konfigurationselement gelesen und geändert werden. Wenn ein snmpset-Befehl mit der Zeichenkette „uci <command> config-item=new-value" ausgeführt wird, markiert er das Config-Item. Der nächste snmpget-Aufruf mit ‚1.3.6.1.4.1.2021.8.1.2.108' (uci_get) merkt sich das letzte Config-Item und gibt den aktuellen Wert zurück (Read-back-Funktion). Wurde das snmpset ohne den String-Teil „=new-value" ausgeführt, wird nur der Config-Item-Marker gesetzt. Dies kann zum Auslesen eines Items (keine OID) verwendet werden, ohne es zu verändern.

Hinweis: Denken Sie daran, die Änderungen mit dem Befehl *uci commit* zu speichern.

7.7.3.1 Neuen Hostnamen festlegen

Der Hostname ist in ‚/etc/config/system' konfiguriert (keine OID).

Die Befehle

```
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
```

liefern

```
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 = ""
```

Verwenden Sie die folgende Reihenfolge, um den neuen Hostnamen einzustellen

```
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 Erstellen eines Beschreibungstexts für die Systemkonfiguration

Die reguläre Firmware-Konfiguration stellt solche Informationen nicht zur Verfügung. Die folgende Befehlssequenz

```
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
```

liefert

```
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 = ""
```

Bestätigen Sie diese Änderung vom UCI-Zwischenspeicher zum permanenten Overlay-Dateisystem.

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

Es ist kein Service-Reload erforderlich.
```

7.7.3.3 Beschreibungstext für die Systemkonfiguration löschen

Die folgende Befehlssequenz

```
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
```

liefert

```
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 = ""
```

Bestätigen Sie diese Änderung vom UCI-Zwischenspeicher zum permanenten Overlay-Dateisystem.

```
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-Applikationen

7.8.1 SNMP-Support für GPS

Die folgende Informationsdatenstruktur kann über den SNMP-Befehl ‚snmpwalk' von einem Host-System bezogen werden.

Der Befehl

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

liefert

```
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

22

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 = ""
```

Die Werte „Latitude DMS" und „Longitude DMS" werden als Hex-Strings zurückgegeben, da sie Anführungszeichen und doppelte Anführungszeichen enthalten.

Diese konvertierte NMEA 0183-Datenstruktur wird mit Standardkonfiguration (nach Werksreset) geliefert. Die Konfiguration kann angepasst werden, um das rohe NMEA 0183-Protokoll zu liefern. Folgende Schritte sind notwendig, um auf das rohe Protokoll umzuschalten.

Öffnen Sie eine Remote-Root-Konsole mit ‚ssh'-Zugang und wenden Sie folgende Befehle an.

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

root@CyBoxAP:/# uci commit

root@CyBoxAP:/# reboot
```

Nach dem Neustart ist das GPS-Subsystem so konfiguriert, dass es rohe NMEA 0183-Daten liefert. Beachten Sie, dass diese Daten nicht in der Weboberfläche angezeigt werden, aber über SNMP ausgelesen werden können (andere OID als umgewandelte GPS-Info).

Der Befehl

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

liefert

```
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 für zweite GPS-Quelle

Bei einigen CyBox AP-Modellen kann das LTE-Modem auch zusätzliche GPS-Informationen liefern. Wenn das Modem-GPS aktiviert ist und eine zusätzliche GPS-Antenne eingesteckt ist, können diese SNMP-OIDs verwendet werden, um weitere GPS-Informationen zu sammeln.

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 DER FLYING CONTROLLER-MECHANISMUS

Einige Aufgaben erfordern Kenntnisse, die in einem einzelnen Netzwerkknoten nicht verfügbar sind. Um z. B. einen „Rogue Access Point“ zu erkennen, müssen alle zum WLAN-Netz gehörenden Access Points bekannt sein, um diejenigen zu identifizieren, die nicht dazu gehören. Außerdem scannen mehrere Access Points die Umgebung, und deren Ergebnisse müssen an einem zentralen Punkt gesammelt und ausgewertet werden. Daher wird im Netzwerk ein einzelner „Controller“ benötigt, der diese Informationen sammelt und dann die unerwünschte AP-Erkennung durchführt.

Der „Flying Controller“ ist ein Algorithmus, der auf mehreren Netzwerkgeräten gleichzeitig ausgeführt wird und eines dieser Geräte als „Controller“ auswählt. Alle anderen Geräte werden als „Worker“ bezeichnet. Fällt der Controller aus, wird ein neuer gewählt, daher der Begriff „fliegend“. Auf diese Weise wird eine zentrale Steuerung aufgebaut ohne einen „Single Point of Failure“ zu schaffen.

Der CyBox AP 2 nimmt automatisch am Mechanismus teil und kann als Controller gewählt werden, ansonsten wird er ein Worker.

Der Wahlmechanismus ist die Grundlage für den 6.1.2.12 Rogue-Access Point-Erkennungsservice . Dieser Dienst wird auf dem Controller ausgeführt und sammelt Daten von den Workern, um Rogue-APs zu erkennen.

Der „Flying Controller“-Mechanismus hat keine Konfigurationsmöglichkeiten.

9 IPSecVPN / StrongSwan

strongSwan ist eine plattformübergreifende IPsec-Implementierung. Der Schwerpunkt des Projekts liegt auf starken Athentifizierungsmechanismen unter Verwendung von X.509 Public-Key-Zertifikaten und der optionalen sicheren Speicherung von privaten Schlüsseln und Zertifikaten auf Smartcards durch eine standardisierte PKCS#11-Schnittstelle und auf TPM 2.0.

Detaillierte Informationen über die **strongSwan IPsec**-Implementierung finden Sie hier:

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

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

9.1 Benutzerdefinierte IPSec-Konfiguration

Bei der Implementierung der LuCi-Weboberfläche „IPSecVPN“ und des OpenWrt-Service-Startups werden drei service-konforme Konfigurationsdateien aus der OpenWrt-Konfigurationsdatei ‘*/etc/config/ipsec*’ generiert.

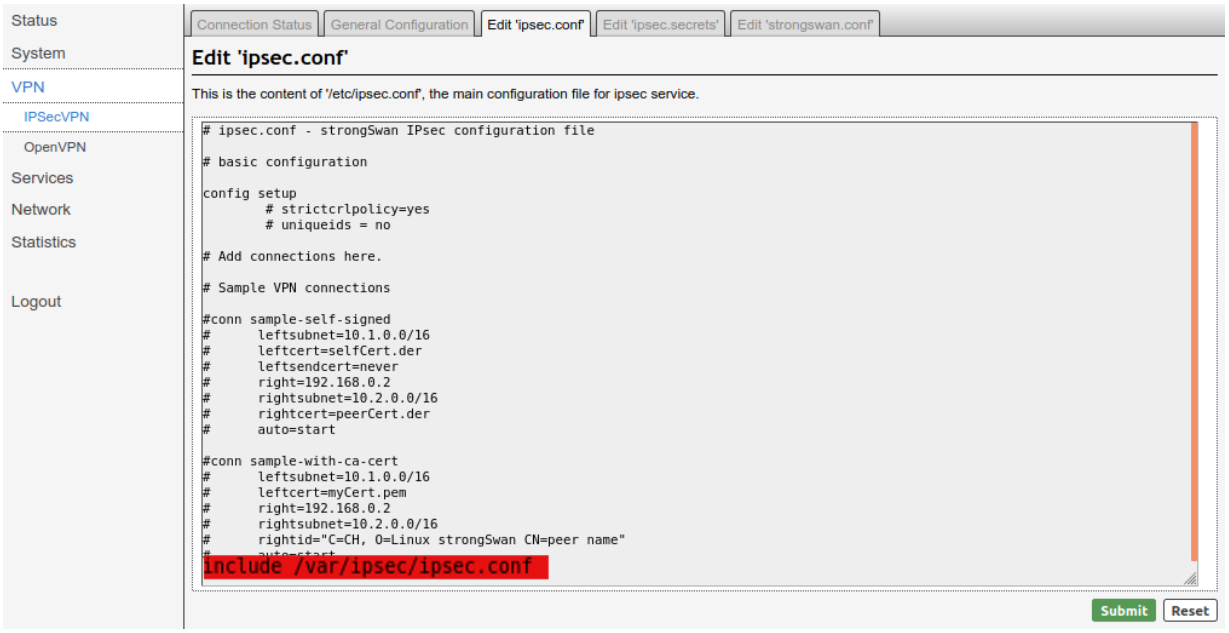
Diese drei Standardkonfigurationsdateien sind:

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

Wenn der IPSec-Service gestartet wird, wird die Konfigurationsdatei ‘*/etc/config/ipsec*’ in drei volatile Konfigurations-Include-Dateien umgewandelt, die sich in ‘*/var/ipsec/*’ befinden.

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

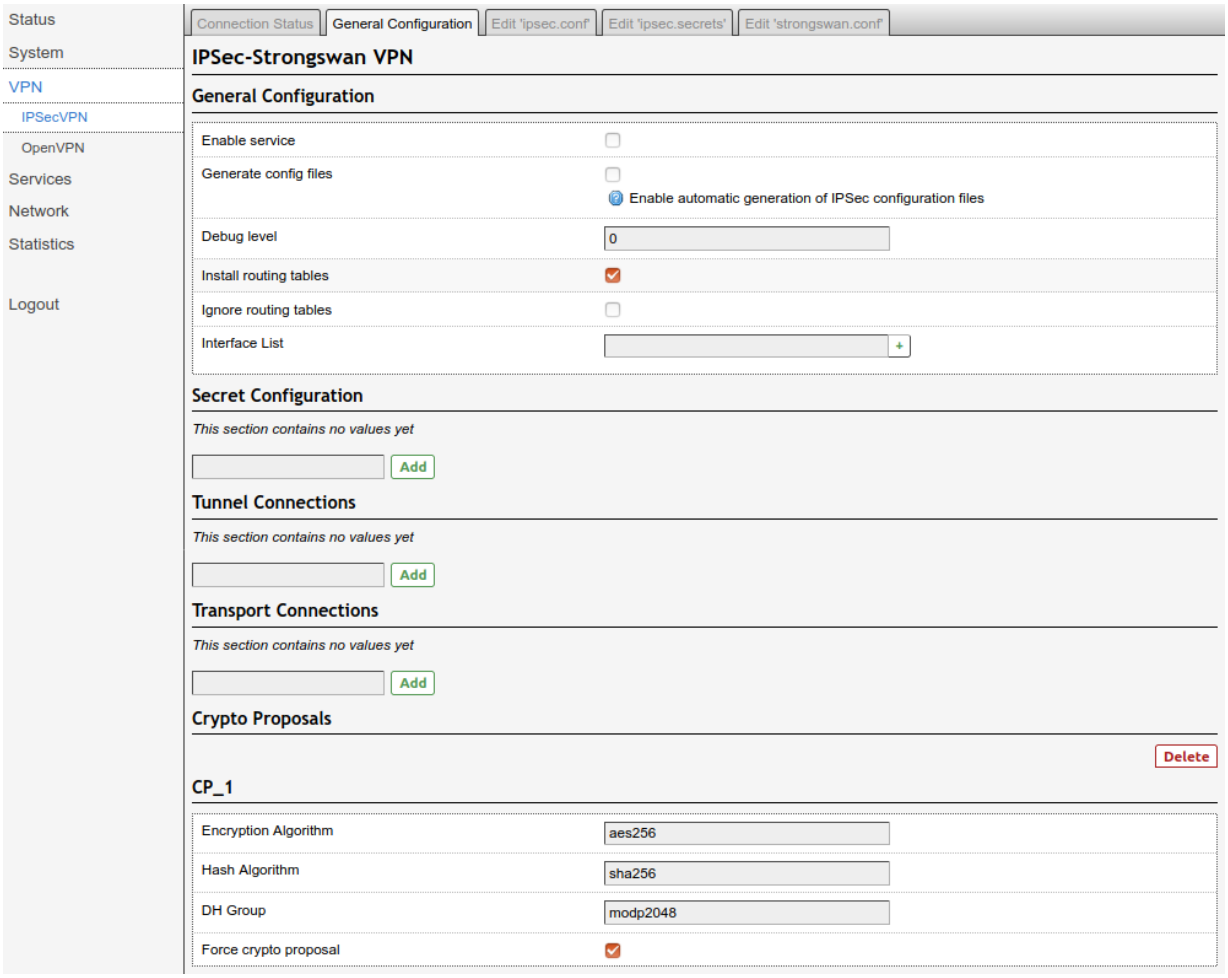
Die drei Standard-Konfigurationsdateien enthalten die generierten Dateien, können aber auch auf der IPSecVPN-Webseite mit dem entsprechenden Menü-Editor angepasst werden.



IPSec-Service-Konfigurationsdateien können bearbeitet (angepasst) werden

9.2 IPSec-Standardkonfiguration

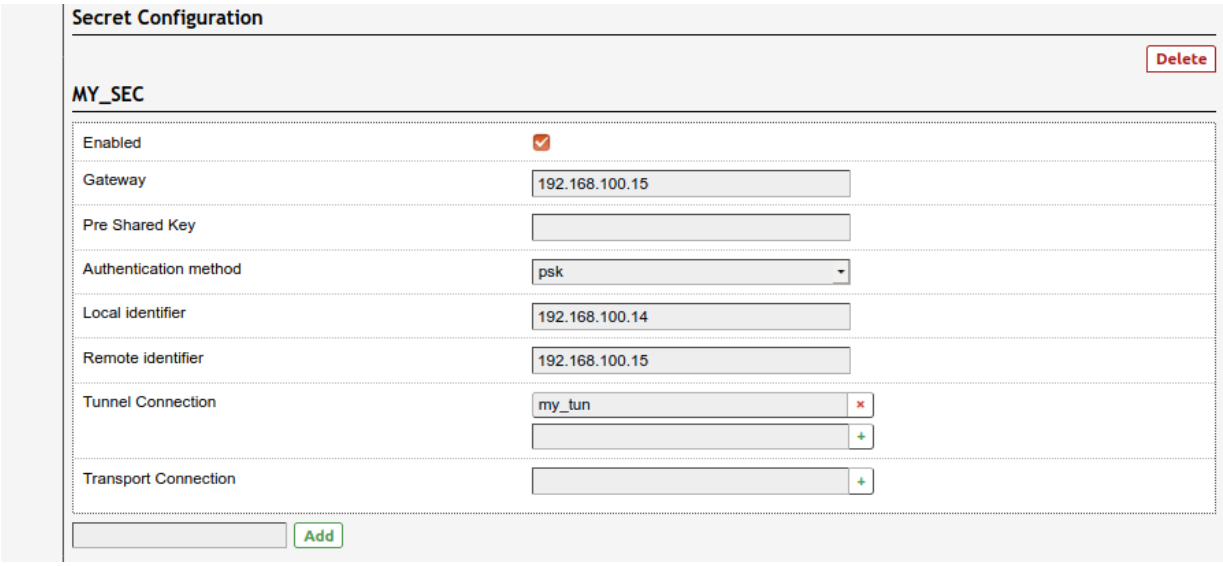
Der Service ist in der werkseitigen Standardkonfiguration deaktiviert. Der erste Schritt besteht darin, zu entscheiden, ob Konfigurationsdateien automatisch generiert oder vom Bediener bereitgestellt und bearbeitet werden sollen. In den nächsten Kapiteln wird davon ausgegangen, dass die Konfiguration vom IPSec-Startskript (`init.d/ipsec`) generiert wird.



IPSec-Werkseinstellung

9.3 IPSec-Geheim-Konfiguration

Die Datei `ipsec.secrets` enthält die Pre-Shared-Keys (*PSK*) für eine zuvor konfigurierte `Tunnel`- und/oder `Transport`-Verbindung. Die *PSK* ist die einzige unterstützte Authentifizierungsmethode.

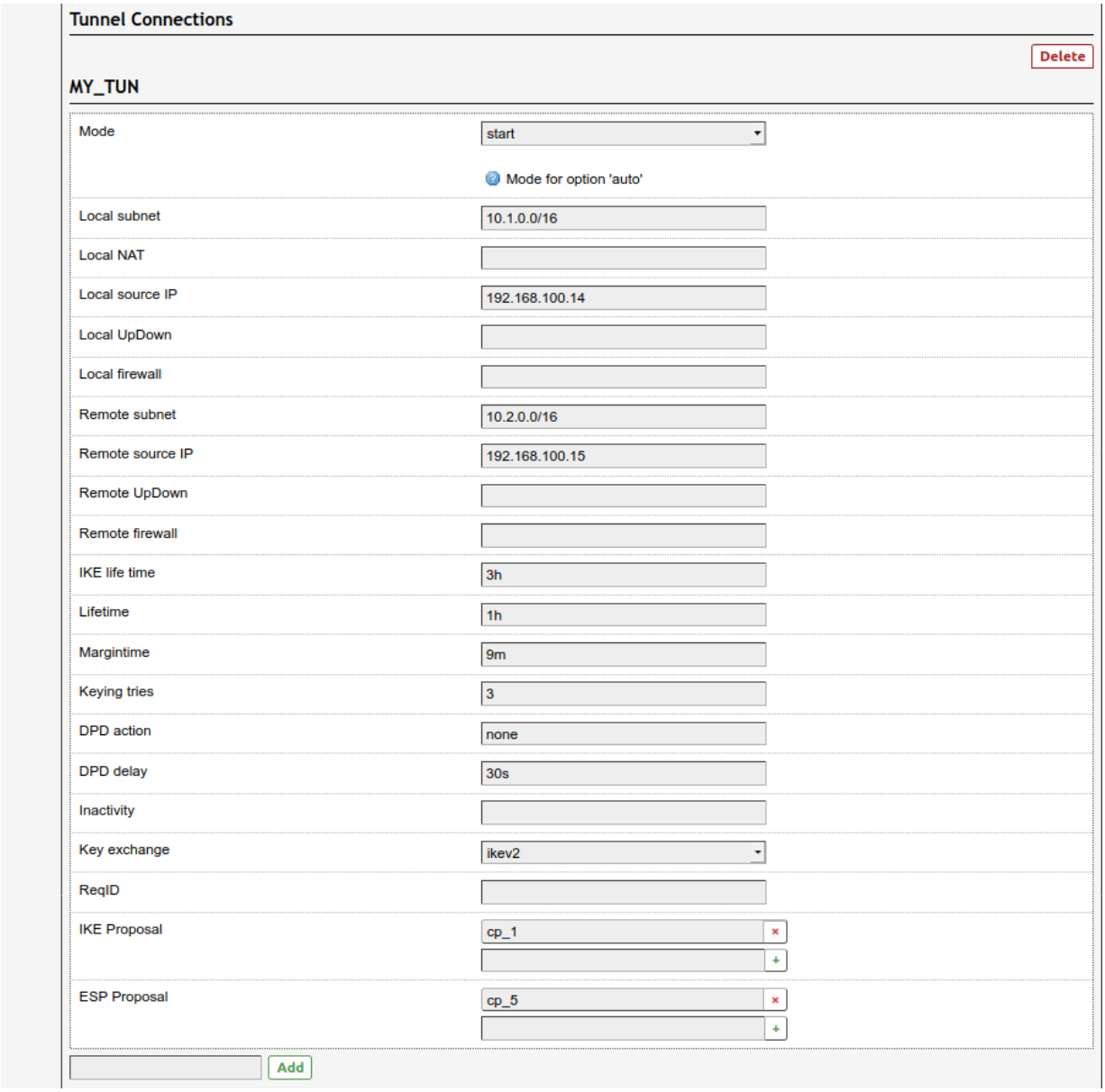


PSK-Geheim-Konfiguration

9.4 IPSec Tunnel/Transport-Verbindung

Die Parameter in diesem Menü sind analog zu den Standardparametern in der offiziellen Konfigurationsdokumentation benannt. Bitte beziehen Sie sich auf:

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



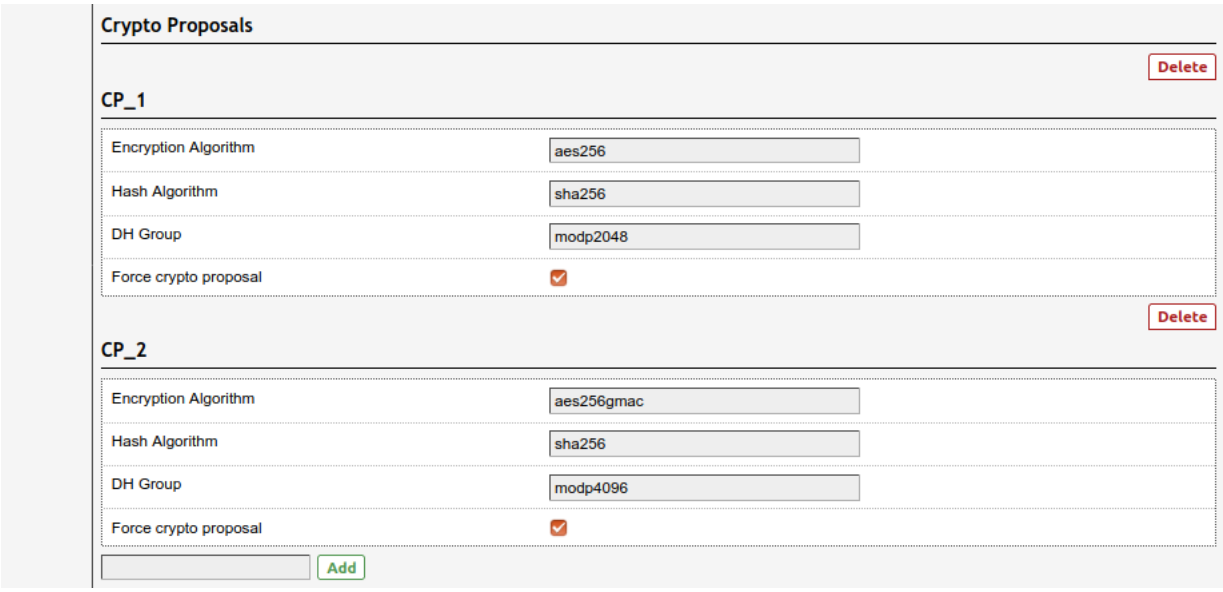
Konfiguration der Tunnel-Verbindung

Die Transport-Verbindung ähnelt dem Setup der Tunnel-Verbindung.

Konfiguration der Tunnel-Verbindung

9.5 IPSec-Crypto-Proposal-Konfiguration

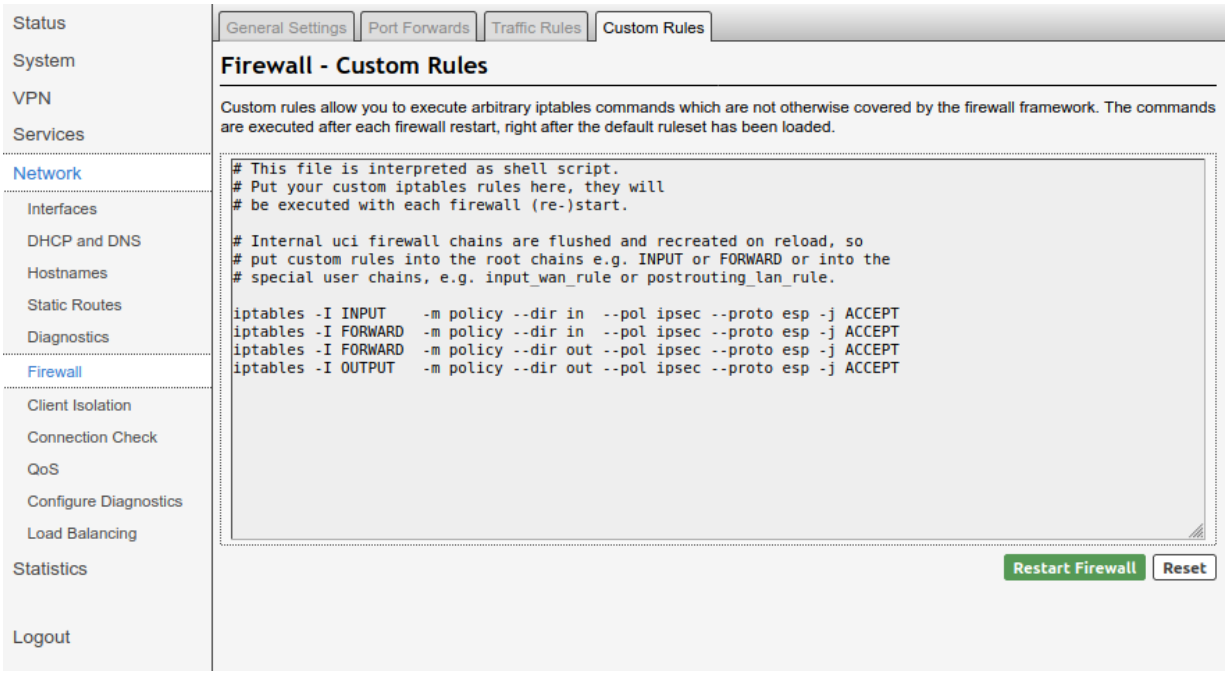
In der Standard-Werkskonfiguration sind bereits einige Crypto Proposals definiert. Mit der Schaltfläche `Add` können neue Vorschläge hinzugefügt werden. Mit der Schaltfläche `Delete` können nicht benötigte Crypto-Proposals aus der Konfiguration entfernt werden.



Krypto-Proposals, einige sind vordefiniert

9.6 Benutzerdefinierte IPSec-Firewall-Regeln

Das Standard-Firewall-Setup (Werkseinstellung) erfordert möglicherweise neue benutzerdefinierte Regeln für die Weiterleitung von IPSec-ESP-Paketen.



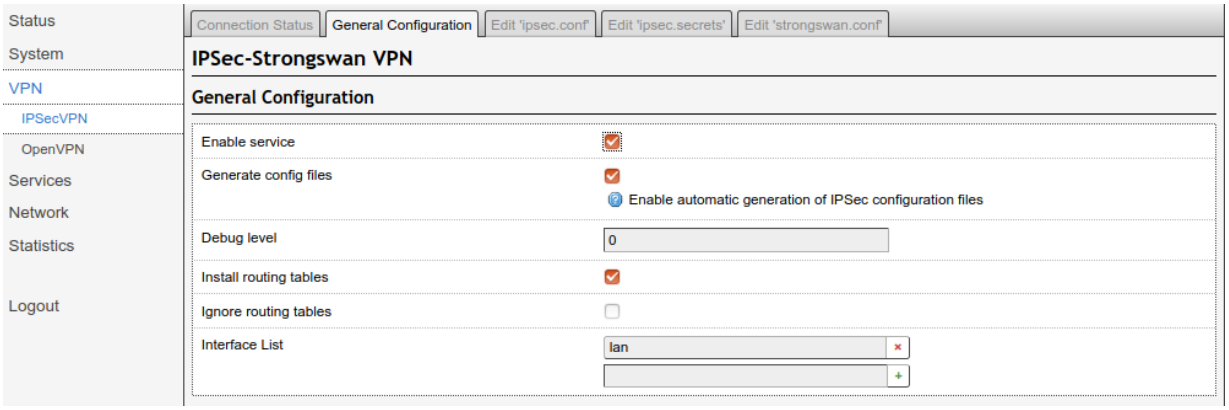
Die Firewall hat einige zusätzliche benutzerdefinierte Regeln

„Cut and Paste“-Puffer für IPSec `Firewall - Custom Rules` bearbeiten:

```
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
```

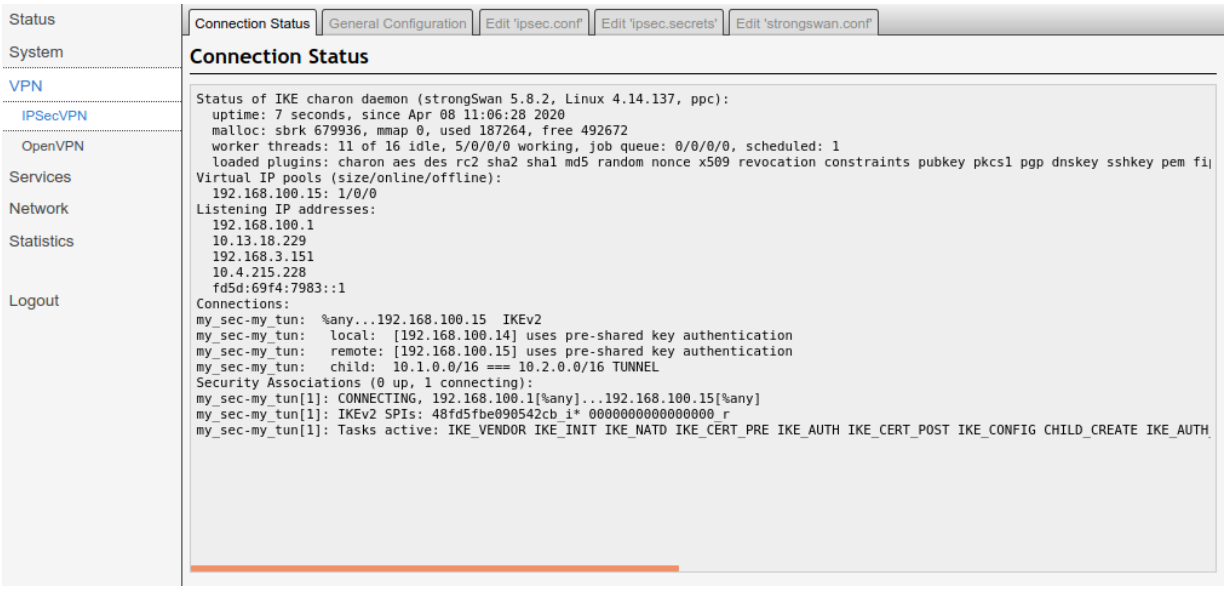
9.7 IPSec-Service-Start

Wenn das Feld `Enable service` aktiviert ist und neue Einstellungen übernommen werden, wird der Service neu gestartet.



Der IPSec-Service wird automatisch neu gestartet

Der Verbindungsstatus des IPSec-Services kann im Menüreiter `Connection Status` beobachtet werden.



Status des IPSec-Dienstes, der auf die Verbindung wartet

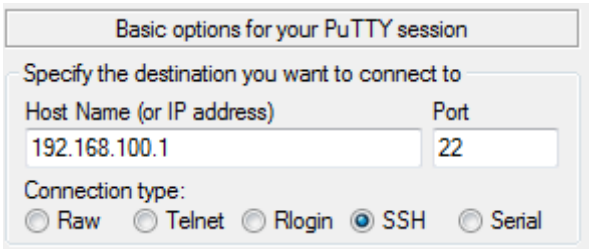
10 SSH / SERIELLE KONSOLE

Auf einem Windows-PC können Sie das Programm PuTTY (http://www.putty.org) verwenden.

a. Ethernet-Kabel (SSH)

Stellen Sie sicher, dass ein Ethernet-Kabel zwischen Ihrem PC und dem Access Point angeschlossen ist. In der folgenden Anweisung wird davon ausgegangen, dass die Standardeinstellungen verwendet werden.

- Wenn Sie einen UNIX/Linux-PC verwenden, führen Sie den Befehl 'ssh root@192.168.100.1' aus.
- Wenn Sie einen Windows-PC verwenden, sollte PuTTY wie folgt konfiguriert werden:

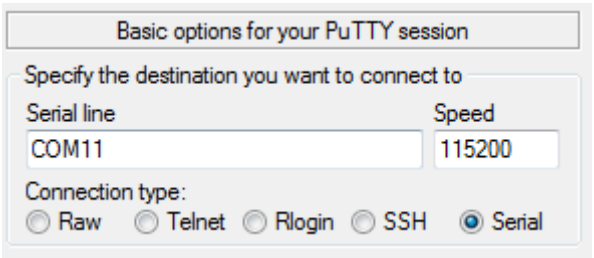


PuTTY - SSH-Verbindung

b. Serielles Kabel

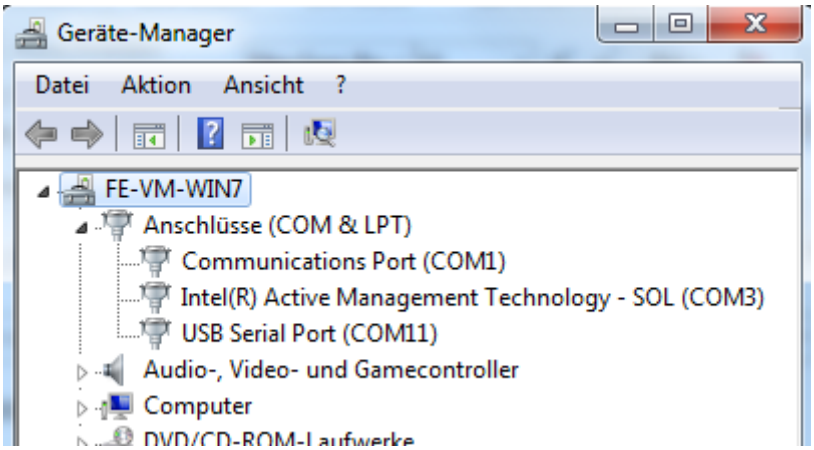
Stellen Sie sicher, dass ein serielles Kabel zwischen Ihrem PC und dem Access Point angeschlossen ist (ein spezieller CyBox-Adapter, der in den USB-Anschluss gesteckt wird, ist erforderlich).

- Installieren Sie auf einem UNIX-PC das Programm picocom, und führen Sie den Befehl picocom -b 115200 /dev/ttyUSB0 (*'ttyUSB0'* muss geändert werden abhängig von Ihrem PC) aus.
- Wenn Sie einen Windows-PC verwenden, sollte PuTTY wie folgt konfiguriert werden:



PuTTY - Serielle Verbindung

Der Wert *'COM11'* muss für Ihren PC angepasst werden. Eine Liste der COM-Anschlüsse finden Sie im Geräte-Manager-Fenster (siehe unten).



Windows-Geräte-Manager mit COM-Anschlüssen

Sobald die Verbindung hergestellt ist, sollte eine Anmeldung im seriellen Konsolenfenster angefordert werde.

Ist dies nicht der Fall, drücken Sie die Enter-Taste auf der Tastatur und/oder trennen Sie den seriellen USB-Adapter an der Seite der CyBox und schließen Sie ihn wieder an. Zum Bearbeiten von Dateien auf dem Zielsystem kann der integrierte Texteditor **nano** verwendet werden.

10.1 UCI-Konfiguration

Dieser Abschnitt beschreibt die UCI (**Unified Configuration Interface**). UCI kann für die Remote-Konfiguration mithilfe von Shell-Befehlen und -Skripten als Skript erstellt werden. UCI kann als OpenWRT-Hauptkonfigurationsschnittstelle angesehen werden. Es wird eingesetzt für die Konfiguration der Hauptnetzwerkschnittstelle, die WLAN-Einstellungen, die Protokollierungsfunktionen und die RAS-Konfiguration.

Mit OpenWrt sollte der Benutzer nur UCI-Konfigurationsdateien ändern, die von einzelnen Programmen gelesen werden.

Eine ausführlichere Beschreibung der verwendeten UCI-Befehle und -Dateien finden Sie unter https://wiki.openwrt.org/doc/uci.

10.1.1 UCI-Konfigurationsdateien

Die zentrale OpenWRT-Konfiguration ist in mehrere Dateien aufgeteilt, die sich im Verzeichnis /etc/config/ befinden. Jede Datei wird nach dem Teil des Systems benannt, den sie konfiguriert. Die Konfigurationsdateien können entweder mit einem Texteditor oder mit UCI geändert werden. UCI-Konfigurationsdateien können auch über verschiedene Programmier-APIs (wie Shell, Lua und C) geändert werden. Auf diese Weise nehmen Webschnittstellen wie LuCI Änderungen an den UCI-Dateien vor.

Nach dem Ändern einer UCI-Konfigurationsdatei müssen die betroffenen Services durch einen Aufruf von init.d neu gestartet werden, damit die aktualisierte UCI-Konfiguration verwendet wird. Viele Programme werden mit UCI kompatibel gemacht, indem das Skript init.d ihre programmspezifischen Standardkonfigurationsdateien schreibt. Das Skript init.d schreibt zuerst die Konfigurationsdatei an den von der Software erwarteten Speicherort und wird durch einen Neustart der ausführbaren Datei erneut eingelesen. Beachten Sie, dass ein direktes (erneutes) Starten der ausführbaren Datei ohne init.d-Aufrufe nicht zu einem UCI-Update führt. Änderungen an Dateien in /etc/config/ werden dann nicht wirksam.

10.1.2 UCI-Beispiel

Angenommen, Sie möchten die IP-Adresse des Geräts von 192.168.100.1 auf 192.168.2.1 ändern. Ändern Sie die Zeile in der Datei `/etc/config/network`:

```
option ipaddr 192.168.100.1
```

nach:

```
option ipaddr 192.168.2.1
```

Übernehmen Sie als Nächstes die Einstellungen, indem Sie folgenden Befehl ausführen:

```
/etc/init.d/network restart
```

Denken Sie daran, sich erneut bei der neuen IP-Adresse anzumelden.

10.2 Andere Befehle

a. Stellen Sie die Werkseinstellungen wieder her

   Die Werkseinstellungen können mit dem Befehl factory_reset wiederhergestellt werden.

b. Exportieren der Konfiguration

   Die aktuelle Konfiguration kann im CyBox-Ordner *'/tmp/'* mit dem Befehl `sysupgrade -b /tmp/backup<mybackupname>.tar.gz` gespeichert werden. Sie kann dann mit SCP (oder dem Programm WinSCP für Windows) auf einen PC exportiert werden.

c. Importieren der Konfiguration

   Stellen Sie die Werkseinstellungen wieder her und importieren Sie Ihre archivierte Konfiguration mit SCP (oder WinSCP) nach *'/tmp/'*. Die Konfiguration kann mit dem Befehl `sysupgrade -r /tmp/backup-<mybackupname>.tar.gz ; reboot` installiert werden.

Wenn Sie in der Befehlszeile reboot eingeben, wird das Gerät neu gestartet.

Der USB-Stick wird automatisch an /mnt/sda1 angeschlossen.

11 SYSTEMWARTUNG

11.1 Remote-Firmware-Upgrade

Die Flash-Partition *standard_boot*, die das binäre Standard-Firmware-Image (.itb-Image) enthält, kann remote aktualisiert werden. Das neue Firmware-Image muss mit dem Befehl **scp** auf das Zielsystem kopiert werden. Anschließend werden durch **ssh**-Aufrufe lokale Zielprogramme ausgeführt, um die neue Firmware zu installieren.

Während das OpenWrt-Betriebssystem ausgeführt wird, kann die Partition *standard_boot* jederzeit beschrieben werden.

Wenn für das Firmware-Update **keine** Konfigurationsänderung erforderlich ist, kann die aktuelle Systemkonfiguration beibehalten werden. Bitte wenden Sie sich an den Support oder den Vertrieb, wenn für Ihr Update ein Reset der Konfiguration von einer älteren auf eine neuere Version erforderlich ist.

Der **Appendix: Script for Remote Firmware Update** enthält ein *Bash*-Script **rsysupgrade.sh**, um den Remote-Update-Prozess von einer Linux-Host-Konsole zu demonstrieren.

11.1.1 Remote-Firmware-Upgrade ohne Konfigurationsänderung

Normalerweise sollte ein Firmware-Update auch ein Zurücksetzen der Konfiguration auf die neue Version beinhalten. Nur in einigen wenigen Fällen, z.B. für eine kleine Fehlerbehebung in einem WLAN-Treiber, ist es nicht erforderlich, ein neues Konfigurations-Backup-Archiv anzupassen und zu installieren.

Die folgenden Befehle können von einer Linux-Konsole oder mit ähnlichen Windows-**Putty**-Dienstprogrammen ausgeführt werden.

1. Kopieren Sie das neue Firmware-Image auf das Zielsystem

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

2. Flashen Sie die neue Firmware in die **standard_boot** Flash-Partition (mtd2) und starten Sie das Zielsystem neu

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

11.1.2 Remote-Firmware-Upgrade mit neuer Konfiguration

In den meisten Fällen muss auch ein angepasstes oder neues Konfigurationsarchiv installiert werden, um der neuen Firmware-Version zu entsprechen. Die Overlay-Partition wird verwendet, um die vom Benutzer vorgenommenen Konfigurationseinstellungen nach dem Aus- und Einschalten es Geräts verfügbar zu halten. Wenn die Firmware eine leere (gelöschte) Overlay-Partition erkennt, wird das Zielverzeichnis **/mnt/custom/** auf ein einzelnes **backup-<target>-<cfg>.tar.gz**-Archiv geprüft, das als neue Konfiguration installiert werden soll. Wenn ein **/mnt/custom/backup-<target>-<cfg>.tar.gz**-Archiv **nicht** existiert, werden die „Werkseinstellungen“ angewendet.

Um Ihre benutzerdefinierte Konfiguration für eine neue Firmware zu erstellen, sollte die alte Systemfirmware auf die neue Version mit gelöschter Konfiguration und den `Werkseinstellungen` aktualisiert werden. Erstellen Sie Ihre vollständige System-Konfiguration mit der neuen Firmware-Version und speichern Sie das Archiv **backup-<target>-<cfg>.tar.gz** auf Ihrem Host-System. Das hochgeladene Backup-Archiv kann dann auf andere (stationäre) Ziele exportiert werden, die mit den gleichen Hardwarekomponenten ausgestattet sind.

Die folgenden Befehle können von einer Linux-Konsole oder mit ähnlichen Windows-**Putty**-Dienstprogrammen ausgeführt werden.

1. Kopieren Sie das neue Firmware-Image auf das Zielsystem

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

2. Flashen Sie eine neue Firmware auf die Flash-Partition **standard_boot** (mtd2)

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

3. Stellen Sie sicher, dass keine Sicherungskonfiguration in **/mnt/custom/** gespeichert ist

```
ssh  root@<target_ipv4>: "rm -rf /mnt/custom/backup*"
```

4. Optional können Sie Ihre neue benutzerdefinierte Konfiguration nach `/mnt/custom/` exportieren. *Hinweis* Das Zielsystem führt einen zusätzlichen Neustart durch, um Ihre neue Konfiguration zu aktivieren. Wenn keine Konfiguration exportiert wird, wird automatisch die Standardkonfiguration der neuen Firmware angewendet.

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

5. Löschen Sie die aktuelle Konfiguration und starten Sie neu:

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

WARNUNG: Schalten Sie den Access Point NICHT AUS, während Sie die Firmware auf Flash aktualisieren/wiederherstellen

11.2 USB-Möglichkeiten

Über einen USB-Stick ist es möglich, Konfiguration und Firmware zu aktualisieren.

Ein USB-Stick kann an das Gerät angeschlossen werden, er benötigt einen speziellen USB-Adapter.

a. Exportieren der Konfiguration

Archivierte Konfigurationen können über die Kommandozeile auf einen leeren USB-Stick exportiert werden, indem die Konfiguration nach *'/mnt/sda1'* kopiert wird.

b. Importieren der Konfiguration

Um eine archivierte Konfiguration in den Access Point zu importieren, warten Sie, bis der Boot-Vorgang abgeschlossen ist, und schließen Sie dann einen USB-Stick an, auf dem sich eine Konfigurationsdatei mit dem Namen *backup-<mycustomname>.tar.gz*' befindet. Auf dem Stick dürfen keine anderen Dateien oder Ordner vorhanden sein. Nach dem Anschließen wird die Konfiguration automatisch eingelesen und es werden nacheinander zwei Neustarts durchgeführt, um Ihre Einstellungen zu übernehmen. Der USB-Stick kann zu Beginn einer Boot-Phase (wenn alle LEDs ausgeschaltet sind) oder nach Abschluss der Boot-Sequenz sicher entfernt werden.

Ein USB-Hotplug-Skript wird ausgelöst, wenn der USB-Stick nach dem Booten eingesteckt ist. Es liest das Stammverzeichnis des Sticks aus und prüft auf eine Liste bekannter Dateitypen:

Dateien auf dem Upgrade-USB-Stick:

File-Typ (wildcard=*)	Beschreibung	Board	Aktion	Wer ?
„backup*tar.gz“	Neues Konfigurationsarchiv	ALL	Untar to Overlay FS (/dev/mtd3)	Endandwender
„factory*reboot“	Markierung, um nach dem Upgrade-Vorgang Werksreset und Neustart durchzuführen	ALL	factory_reset durchführen	Endandwender
„config*reboot“	Markierung zum Ausführen normalen Neustarts	ALL	Reboot durchführen	Endanwender
„cyap*upgrade*tgz“ „cyap*upgrade*zip“	Das Upgrade-Archiv muss ein 'install.sh'-Script (ausführbar) im Stammverzeichnis des Archives enthalten. Das Archiv wird nach /tmp/usb_upgrade endpackt, 'install.sh' wird ausgeführt.	ALL	Ausführen von Shell-Skripten	System-Integrator

Jede Installation wird für jede Datei auf dem USB-Stick nur einmal ausgeführt; bereits installierte Updates werden nicht erneut versucht. Prüfen Sie *'System Log'* in der Weboberfläche oder logread auf der Konsole auf Upgrade-Meldungen.

Für ein Firmware-Upgrade mit dem Archiv *.zip sollte der USB-Stick nur eine Archivdatei im USB-Stammverzeichnis bereitstellen:

Beispiel:

cyap-upgrade-V20.36.3.zip

Diese Upgrade-Archivdatei muss das neue Firmware-Image *V20.36.3-cyap2-lzma.itb* und ein ausführbares Installationsskript namens *install.sh* enthalten. Das Installationsskript führt Befehle aus, um die neue Firmware in die gewünschte Partition zu flashen. Das Upgrade-Archiv kann auch ein Backup-Archiv der neuen Konfiguration enthalten, das für die neue Firmware-Version geeignet ist. Nach dem Firmware-Upgrade kann die neue Konfiguration auch mit Befehlen aus dem Installationsskript angewendet werden.

Beispiel für ein *install.sh*-Script:

```
#!/bin/sh

sysupgrade -t V20.36.3-cyap2-lzma.itb
sysupgrade -r backup-cyap2-20.36.3.tar.gz

exit 0
```

11.3 Status der LED-Blink-Codes

Während der Upgrade-Prozess läuft oder beendet ist, dient die 'Fail LED' (rot/grün) als Statusanzeige.

Blink-Codes in Upgrades:

Blink-Code wiederholt	Beschreibung
ROT 0,2 sec an - GRÜN 0,2 sec an	Upgrade-Prozess läuft
GRÜN durchgehend an	Upgrade erfolgreich
ROT durchgehend an	USB-Stick-Anschluss fehlgeschlagen
ROT 3 sec an - AUS 0,5 sec	Overlay-FS-Anschluss fehlgeschlagen
GRÜN 3 sec an – AUS 0,5 sec	Ein Upgrade läuft bereits
ROT 0,2 sec – AUS 0,5 sec – ROT 0,2 sec – AUS 2 sec	Kopieren ins Flash fehlgeschlagen
ROT 0,2 sec – AUS 0,5 sec – ROT 0,2 sec – AUS 0,5 sec – ROT 0,2 sec AUS 2 sec	'install.sh' fehlt
GRÜN 0,2 sec – AUS 0,5 sec – ROT 0,2 sec – AUS 0,5 sec – ROT 0,2 sec - AUS 0,5 sec	Passwort fehlt
GRÜN 0,2 sec – AUS 0,5 sec – ROT 0,2 sec – AUS 0,5 sec – ROT 0,2 sec - AUS 0,5 sec – ROT 0,2sec - AUS 0,5sec	Passwort ungültig
OFF	USB-Stick wurde entfernt

12 ANHANG: GPL-LIZENZ

```
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.

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

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.

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.

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,

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.

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.

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 ANHANG: SNMP-OID-ÜBERSICHT

Diese Übersicht ist auch im Auslieferungszustand erhältlich über die Weboberfläche unter Verwendung der 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
```

```
custom1 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 ANHANG: STANDARD-WERKSEINSTELLUNGEN

Im Auslieferungszustand verfügt das Gerät über die folgenden Standardeinstellungen:

Standardeinstellungen für Ethernet 1 (alle Modelle):

Interface	IPV4 Adresstyp	Adresse	Bemerkung
lan	Statische IPv4 Adresse	192.168.100.1/24	
lan_alias	Statische IPv4 Adresse	Berechnet basierend auf Seriennummer	Siehe Kapitel 4.1 IP-Adressen der CyBox AP 2
lan_dhcp	IPv4 DHCP Client		
lan_mac	Statische IPv4 Adresse	Berechnet basierend auf eth0 MAC-Adresse	Siehe Kapitel 4.1 IP-Adressen der CyBox AP 2

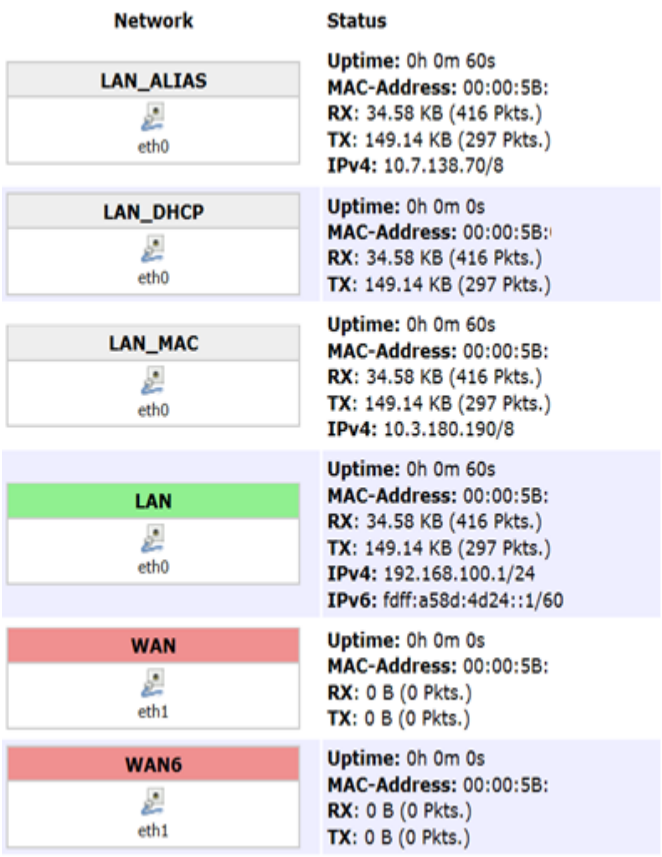
Standardeinstellungen für Ethernet 2:

Interface	IPV4 Adresse	Adresse	Bemerkung
wan	IPv4 DHCP Client		
wan6	IPv6 DHCP Client		

Andere Standardeinstellungen (alle Modelle):

Interface	Parameter	Bemerkung
Passwort für User ‘Root’	Root	Stellen Sie sicher, dass Sie es vor dem Einsatz ändern
WLAN, LTE, GPS	deaktiviert	
Bridge	deaktiviert	
DHCP/DNS Server	deaktiviert	

Firewall	*'Input'* und *'Output'* sind auf *ACCEPT*, *'Forward'* auf *REJECT* gesetzt	
VLAN	Nicht konfiguriert	



Standard-Netzwerkkonfiguration